★ VIRGINIA ★
STATE BOARD of ELECTIONS

BOARD MEETING

Monday, November 18, 2019
West Reading Room
Patrick Henry Building
Richmond, VA
1:00 P.M.

SBE Board Working Papers

STATE BOARD OF ELECTIONS
AGENDA

DATE: Monday, November 18, 2019
LOCATION: Patrick Henry Building
West Reading Room
1111 E. Broad Street
Richmond, VA
TIME: 1:00 PM

I. CALL TO ORDER

Robert Brink, Chairman

II. COMMISSIONER'S REPORT

Christopher E. Piper
Commissioner

III. GENERAL ELECTION CERTIFICATION

Matt Abell
Elections Administration

IV. EARLY VOTING REPORT

Danny Davenport
Policy Analyst

V. STAND BY YOUR AD

Arielle A. Schneider
Policy Analyst

1. **Andy Cullip For Pulaski County BOS**
2. **Arika Phillips For CCPS School Board**
3. **Charon Coffee Price_Lunenburg County Commissioner of the Revenue**
4. **Chris Peace for Delegate**
5. **Darby McGeorge**
6. **Darryl V. Parker**
7. **David Hardin**
8. **Friends of Virginia Smith**
9. **Gerald Mitchell Williamsburg_James City County Sheriff**
10. **Gilbert Smith Charles City County BOS**
11. **Hallahan for Supervisor**
12. **Joe Dombrowski_ New Kent County BOS**
13. **John Edward Hall**
14. **John Whitbeck for Chair**
15. **Lyndsey Dotterer**

16. **Missy Cotter Smasal_8th Senate District**
17. **Partnership for New Kent PAC**
18. **Paul Petrauska_Fauquier County BOS**
19. **Ralph Parham**
20. **Reginald Williams**
21. **Samantha Bohannon (CC-19-01091)**
22. **Scott Mayausky_Commissioner of the Revenue Stafford County**
23. **Starla Kiser for Delegate**
24. **Stop Trafficking Augusta**
25. **Sue Kass**
26. **Susan Shick**
27. **Tim Hayden**
28. **Tim Mclaughlin**
29. **Wade for Sheriff**
30. **Will Gardner**
31. **Winchester Frederick Democratic Committee**

VI. HB2178 MINIMUM SECURITY STANDARDS

Daniel Persico
Chief Information Officer

VII. PUBLIC COMMENT

VIII. ADJOURNMENT

★ VIRGINIA ★
STATE BOARD of ELECTIONS

Commissioner's Report

BOARD WORKING PAPERS
Christopher E. Piper
Commissioner

★ VIRGINIA ★
STATE BOARD *of* ELECTIONS

General Election Certification

BOARD WORKING PAPERS
Matt Abell
Elections Administration

★ VIRGINIA ★
STATE BOARD of ELECTIONS

Memorandum

To: Chairman Brink, Vice Chair O'Bannon, and Secretary LeCruise

From: Matthew Abell, Elections Administrator

Date: November 18, 2019

Re: Certification of Results for the November 5, 2019 General and Special Elections

Suggested Motion For A Board Member To Make:

"After reviewing the abstracts of votes cast in the November 5, 2019 General and Special Elections, I move that the Board certify the results as presented by signing said abstracts and the certificates of election."

Applicable Code Sections:

- Va. Code § 24.2-679.A. "The State Board shall meet on the third Monday in November to ascertain the results of the November election. …The Board shall… make statements of the whole number of votes given at any such election for members of the General Assembly, …and any officer shared by more than one county or city, or any combination thereof, or for so many of such officers as have been voted for at the election. … The Board members shall certify the statements to be correct and sign the statements. The Board shall then determine those persons who received the greatest number of votes and have been duly elected to each office. The Board members shall endorse and subscribe on such statements a certificate of their determination."

- Va. Code § 24.2-680 "Subject to the requirements of § 24.2-948.2, the State Board shall without delay complete and transmit to each of the persons declared to be elected a certificate of his election, certified by it under its seal of office. …The names of members elected to the General Assembly shall be certified by the State Board to the clerk of the House of Delegates or Senate, as appropriate. … The name of any officer shared by more than one county or city, or any combination thereof, shall be certified by the State Board to the clerk of the circuit court having jurisdiction in each affected county or city. The names of the persons elected to soil and water conservation districts shall be certified by the State Board to the Director of the Department of Conservation and Recreation."

Attachments:

Abstracts of Votes and winner Certificates of Election for the November 5, 2019 races that must be certified by the Board:

- Member, Senate for Virginia – 40 districts
- Member, Virginia House of Delegates – 100 districts
- Shared constitutional offices – 27 total
  - Clerk of Court – 1
  - Commonwealth's Attorney – 13
  - Sheriff – 12
  - Treasurer – 1

Background:

- Upon completion of the election, local general registrars (GRs) entered all relevant election data into the Virginia Election and Registration System (VERIS).

- In accordance with Va. Code § 24.2-671, within seven days after the election, local electoral boards conducted provisional ballot meetings and canvasses to ascertain and certify election results for their localities.

- Upon completion of canvass the GRs forwarded their localities' certified Abstracts of Votes (Abstracts) and, when applicable, Write-Ins Certifications, to the Department of Elections (ELECT).

- To ensure accuracy of the results, ELECT staff performed the procedures below. Staff worked with localities to resolve and/or explain any issues identified. ELECT staff:
  - Confirmed all required Abstracts and Write-In Certifications were properly completed and submitted;
  - Compared turnout to votes cast; and,
  - Compared results listed in the Abstracts and Write-In Certifications to the results entered in VERIS.

ELECT Staff Recommendation:

ELECT staff recommends that the Board vote to certify the results of the November 5, 2019 General and Special Elections as presented and sign the abstracts of votes cast and certificates of election.

★ VIRGINIA ★
STATE BOARD *of* ELECTIONS

Early Voting Report

BOARD WORKING PAPERS
Danny Davenport
Policy Analyst

★ VIRGINIA ★
DEPARTMENT *of* ELECTIONS

Memorandum

To: Chairman Brink, Vice-Chair O'Bannon, and Secretary LeCruise
From: Danny Davenport, Policy Analyst
Date: November 18, 2019
Re: Report on Conducting Absentee Voting

Suggested Motion

"I move the State Board of Elections approve the report as presented and direct the Department of Elections to submit the report to the Governor, General Assembly, and the House and Senate Committees on Privileges and Elections on behalf of the Board."

Background

During the 2019 Session, the General Assembly passed and the Governor signed into law HB 2790/SB 1026 relating to implementing a period of no-excuse, in-person absentee voting beginning with the General Election to be held in November 2020. The law included a clause that the State Board of Elections submit a report to the Governor, General Assembly, and the House and Senate Committees on Privileges and Elections for conducting absentee pursuant to the new law.

Attachments

- Absentee Voting Report

★ VIRGINIA ★
STATE BOARD
of ELECTIONS

Absentee Voting Report

November 12, 2019

Executive Summary

In accordance with the provisions of Chapters 668 and 669 of the 2019 Acts of Assembly (the Act), which reads,

> *"That the State Board of Elections, on or before December 1, 2019, shall submit a report to the Governor, the General Assembly, and the House and Senate Committees on Privileges and Elections on the procedures and instructions promulgated by it for conducting absentee voting pursuant to the provisions of this act. The report shall include recommendations to be considered by the General Assembly for any further legislation that may be necessary for implementation of this act."*

the State Board of Elections is pleased to provide to the Governor, the General Assembly, and the House and Senate Committees on Privileges and Elections this report on the procedures and instructions for conducting absentee voting pursuant to the provisions of the Act. This report includes recommendations to be considered by the General Assembly, including recommended legislation necessary for the implementation of the provisions of the Act.

The State Board of Elections and the Department of Elections are confident that Virginia will be able to implement the Act effectively and efficiently. The report below will demonstrate that the Act does not make sweeping changes to Virginia's existing absentee voting procedures and instructions. Rather, the addition of no-excuse absentee voting is the newest of many expansions to Virginia's absentee voting program. Further, this report will show that we have learned from the many states before us who have already passed similar laws.

Absentee voting first became a major issue during World War II, at which time Congress passed voting laws related to soldiers overseas.[1] Subsequently, the federal government passed the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) and the Military and Overseas Empowerment (MOVE) Act, which have been instrumental in allowing service members to vote. During the 1980s, California became the first state to allow eligible voters to request absentee ballots for any reason.[2]

The November 2020 General Election will mark the first period in Virginia's history where registered voters may vote absentee without providing an excuse. During their discussions of this Act, members of the legislature referred to this process as "no excuse in person absentee voting." However, the General Assembly should note that many states use the term "early voting" to refer to the same process. In this report, we use the term "early voting" when that is the term that a state uses to describe its no-excuse absentee voting period. The National Conference of State Legislatures, cited on several occasions throughout this report, uses the term "early voting" as a shorthand for each state's period of no-excuse absentee voting.[3]

[1] MIT Election Date and Science Lab, "Voting by mail and absentee voting" accessed on October 1, 2019. Retrieved from https://electionlab.mit.edu/research/voting-mail-and-absentee-voting

[2] Id.

[3] See generally State Laws Governing Early Voting. (2019). Retrieved from https:// http://www.ncsl.org/research/elections-and-campaigns/early-voting-in-state-elections.aspx

Thirty-nine states and the District of Columbia provide some form of no-excuse absentee voting.[4] Virginia and Delaware have recently become the 40th and 41st state to enact legislation that allows for no-excuse absentee voting prior to Election Day.[5]

In preparation for the rollout of Virginia's no-excuse absentee voting, we have researched the laws, business practices, and historical data of other states. For example, in September 2019, representatives from the Virginia Department of Elections (ELECT), the Voter Registration Association of Virginia (VRAV), and the Virginia Electoral Board Association (VEBA), traveled to Mecklenburg County, North Carolina to witness their no-excuse absentee voting first-hand. The representatives of ELECT, VRAV, and VEBA all found this exercise extremely useful, in particular as a way to prepare general registrars for the task of administering no-excuse absentee voting in Virginia.

Leaders at ELECT have participated in a number of phone calls with representatives from other states, to discuss their Information Technology (IT) infrastructures for no-excuse absentee voting. Specifically, ELECT leaders participated in preliminary calls with representatives from Mecklenburg County, North Carolina before visiting their locality. ELECT leaders also participated in conversations with the Metropolitan Washington Council of Governments, which provided ELECT with insight into both Maryland and the District of Columbia's IT setups for early voting.

While the period preceding the November 2020 General Election will mark Virginia's first no-excuse absentee voting period, the Commonwealth has already significantly expanded its pool of eligible absentee voters over the past two decades. The chart below shows the expansion of absentee voting in Virginia from 1998 through today.

Year	Change to Va. Code 24.2-700. Person entitled to vote by absentee ballot
1998	Added excuse 8: "Any duly registered person who is unable to go in person to the polls on the day of the election because of an obligation occasioned by his religion[.]"[6]
2000	Added excuse 9: "Any person who, in the regular and orderly course of his business, profession, or occupation, will be at his place of work for eleven or more hours of the thirteen hours that the polls are open pursuant to § 24.2-603."[7]
2001	Added language to reason 9 that allows voters to count their commute to and from work toward reason 9's hour requirement. "Any person who, in the regular and orderly course of his business, profession, or occupation, will be at his place of work and commuting to and

[4] State Laws Governing Early Voting. (2019). Retrieved from https:// http://www.ncsl.org/research/elections-and-campaigns/early-voting-in-state-elections.aspx

[5] State Laws Governing Early Voting. (2019). Retrieved from https:// http://www.ncsl.org/research/elections-and-campaigns/early-voting-in-state-elections.aspx

[6] Chapter 254 of the 1998 Acts of Assembly

[7] Chapter 378 of the 2000 Acts of Assembly

	from his home to his place of work for eleven or more hours of the thirteen hours that the polls are open pursuant to § 24.2-603."[8]
2002	Changed language in reason 2 to include an individual who temporarily reside outside of the United States. Previously, the excuse included only those individuals regularly employed in a business, profession, or occupation outside of the continental limits.[9]
2009	Added excuse 10: "Any person who is a law-enforcement officer, as defined in § 18.2-51.1; firefighter, as defined in § 65.2-102; volunteer firefighter, as defined in § 27-42; search and rescue personnel, as defined in § 18.2-51.1; or emergency medical services personnel, as defined in § 32.1-111.1."[10]
2010	Added excuse 11: "Any person who has been designated by a political party, independent candidate, or candidate in a primary election to be a representative of the party or candidate inside a polling place on the day of the election pursuant to subsection C of § 24.2-604 and § 24.2-639.[11]
2017	Added reason code 12: "Any person granted a protective order issued by or under the authority of any court of competent jurisdiction."[12]
2019	added Virginia Code § 24.2-701.1(2). "Any registered voter may vote by absentee ballot in person beginning on the second Saturday immediately preceding any election in which he is qualified to vote.[13]

For several decades, Virginia has permitted absentee voting for individuals who will be personal business or vacation on Election Day, active duty armed forces members, individuals attending an institution of higher education who will be absent from their county or city on Election Day, individuals with disabilities, individuals awaiting trial for a misdemeanor, and for individuals primarily responsible for caring for an ill or disabled family member.[14] As shown above, Virginia has a history of expanding its absentee voting practices to make voting more convenient and accessible for its registered voters.

Procedures and Instructions

The implementation of in person no excuse absentee voting is a historic development for Virginia. However, the Governor, the General Assembly, and the House and Senate Committees on Privileges and Elections should

[8] Chapter 631 of the 2001 Acts of Assembly
[9] Chapter 785 and 819 of the 2002 Acts of Assembly
[10] Chapters 405 and 873 of the 2009 Acts of Assembly
[11] Chapter 244 of the 2010 Acts of Assembly
[12] Chapter 631 of the 2017 Acts of Assembly
[13] Chapters 668 and 669 of the 2019 Acts of Assembly
[14] See Va. Code § 24.2-700.

note that the Act passed by the 2019 legislature makes very few changes to the existing processes and instructions for absentee voting. Therefore, the responsibilities of registrars and elections officials will not change significantly because of the new law.

The majority of the changes that the Act creates are found in the new Virginia Code section 24.2-701.1, and these changes apply chiefly to the newly implemented eight-day no excuse in person absentee voting period.

Applications

Any registered voter may vote in their locality during the no-excuse absentee period, which lasts from the second Saturday before any election through the Saturday before the election.[15] In this way, the no-excuse absentee period is similar to Election Day. Just like on Election Day, a voter will need to provide only her name, residence address in the county or city in which she is offering to vote, and one of the forms of identification specified in subsection B of § 24.2-643 of the Virginia Code. This is unlike previous absentee periods, when voters were required to submit absentee ballot applications.

While in-person voters will not have to submit absentee ballot applications during the no-excuse absentee period, absentee ballot applications are still required in certain circumstances. The following groups of voters will still need to submit absentee ballot applications: 1) individuals who vote absentee after the forty-fifth day before an election, but before the no-excuse absentee period; and 2) any individuals who vote mail-in absentee.[16] Therefore, general registrars will need to train staff to understand which absentee voters need to submit absentee ballot applications.

Currently, many general registrars choose to use voters' completed in-person absentee ballot applications as a means of reconciling the number of ballots cast and a list of those who have voted. While this process is voluntary and not required by law, many registrars find the process of comparing the number of ballots to a list of those who have voted very useful administratively. Because no absentee ballot applications are required during the no-excuse in person voting period, general registrars may need to devise a different method for tracking this information.

Voting Centers

Virginia Code § 24.2-701.1(C) discusses "additional locations" that may be available for absentee voting in person. We note that the elections community has begun using a few different terms to refer to these "additional locations." Until recently, the common vernacular for these locations among members of the elections community has been "satellite locations." However, the Department of Elections notes that a number of general registrars have begun to refer to these additional locations as "voting centers," because that term may be more intuitive for voters. The State Board has considered that the term "satellite voting locations" may also be a more intuitive term to use to describe these additional locations. We recommend that the General Assembly consider

[15]See Chapter 669 of the 2019 Acts of Assembly § 24.2-701.1(A)(1)
[16] See Chapter 669 of the 2019 Acts of Assembly § 24.2-701.1(A)(1) and §24.2-701.1(A)(2)

legislation to adopt a common term for these additional locations, with consideration of either “satellite voting locations” or “voting centers.” For this report, we will refer to these additional locations as voting centers.

As awareness of no-excuse absentee voting grows, localities may need to establish additional voting centers to manage the increased absentee voter turnout likely to accompany this law.[17] Localities that establish new voting centers will likely face additional expenses. Even localities with pre-existing voting centers may sustain additional expenses related to administering no-excuse absentee voting. A registered voter who chooses to vote during the no-excuse absentee voting period may cast their ballot at any voting center in their locality, regardless of whether they live in the precinct where that voting center is located.[18] Therefore, general registrars will need to train and prepare staff for increased traffic in the general registrar’s office and at any voting centers operating in their localities.

Subsection 701.1(E) of the new law requires the following: “At least two officers of election shall be present during all hours that absentee voting in person is available and shall represent the two major political parties…” Therefore, registrars are responsible for recruiting and training a sufficient number of officers of election to meet the Code requirement for the entire seven-day period of no excuse voting. Previously, these officers were required to be present only on Election Day.

These voting centers will need to be capable of all of the functions of a precinct polling place, plus some additional capabilities. For example, because all registered voters in a locality will be able to vote at any voting center, each voting center must have sufficient numbers of all ballot styles available. Registrars will need to adopt additional processes and procedures appropriate for their office and locality to accommodate these changes. Localities will also need to consider the number of parking spaces as well as physical space requirements of voting centers. As no-excuse absentee voting becomes more prevalent throughout the Commonwealth, many localities may find themselves requiring additional voting centers and/or more space in the registrar’s office. This means increased spending, and potentially the need for additional equipment including tabulators. Additionally, localities may find the need to increase the number of poll books for checking in voters. This may also increase localities’ burden on physical security. They may need additional methods for securely storing ballots, voting materials, and election equipment. These voting centers will also need to comply with all relevant federal law, including the Americans with Disabilities Act.

Election Security

One of the concerns that has been raised by the Virginia elections community with regards to no-excuse absentee voting is the lack of real-time update options for additional voting centers. During ELECT’s research into the procedures of other states who have implemented no-excuse absentee voting, ELECT has catalogued different states’ best practices for preventing any potential cross-site voting. Although this does not seem to be a prevalent issue for states with no-excuse absentee voting, ELECT is taking all necessary steps to ensure that the

[17] The Voter Registrars Association of Virginia (VRAV) has issued a Voter Turnout Projections User Guide that helps Virginia localities make fact-based projections of likely no excuse absentee turnout. This guide uses historical data from North Carolina’s early voting to inform its projections.

[18] See Chapter 669 of the 2019 Acts of Assembly § 24.2-701.1

proper protections are in place to discourage and ultimately prevent this practice. These best practices are in the process of being incorporated into a new set of formal electronic pollbook (EPB) certification requirements and procedures. They are being drafted to account for the operational needs of the Virginia elections community without weakening the Commonwealth's election security posture. The State Board of Elections has not yet approved the EPB certification standards. However, the State Board of Elections is currently working with vendors to develop EPB certification standards and will publish those standards once they have been adopted.

Recommended Legislation

Pursuant to this Act, the General Assembly has requested that the State Board of Elections provide any recommended legislative changes that are necessary for the implementation of the provisions of the Act. After carefully reviewing our own laws and the laws and data of other states, we respectfully submit the following proposed changes to Virginia law.

Below is a chart summarizing the recommended changes to the Act:

Bill Topic	**Summary**
Technical Changes	• For special elections, absentee voting in person shall be available as soon after the deadline in 701.1(a) as possible. • Absentee ballot applications may be completed either at the general registrar's office or at any of the additional locations for absentee voting.
Voting Centers	• Clarifies that any applicant who is in line to cast his ballot when a voting center closes shall be permitted to cast his ballot on that day. • Shifts the ability to establish voting centers from county or city electoral boards to the governing body of each county and city, by ordinance. • Establishes notice requirements for general registrars when voting centers are established or changed. • Makes voting centers equivalent to the office of the general registrar for the purposes of completing an absentee ballot application in person. • Clarifies the requirements concerning distributing campaign materials during the absentee voting period, with reference to Virginia Code § 24.2-604. (Prohibited activities at polls; notice of prohibited area; electioneering; presence of representative of parties or candidates; simulated elections; observers; news media; penalties).
Timeframe Eligibility	• Would replace excuse-based absentee voting with a full forty-five-day period of no-excuse absentee voting.

Technical Changes

We recommend a change to the language of § 24.2-701.1(A). The language in this subsection applies to "any" election held in the Commonwealth and requires in-person absentee voting to begin forty-five days before Election Day. However, for special elections, there is not always a full forty-five day period between the issuance of a writ of election and Election Day itself. Therefore, we recommend adding language to clarify that, in the case of a special election where the full forty-five days is not possible, no-excuse absentee voting should begin as soon as possible after the forty-five-day deadline. This will ensure that administration of the election is not out of compliance with the law in these cases. Special elections for federal offices should be exempted from this exception.

Our second recommended change concerns the use of locations other than the office of the general registrar (voting centers) in § 24.2-701.1(C). Language for this new subsection was copied from § 24.2-707. When the language was copied into the new subsection, a key sentence was omitted. The sentence read as follows: "Such location shall be deemed the equivalent of the office of the general registrar for the purpose of completing the application for an absentee ballot in person pursuant to §§ 24.2-701 and 24.2-706." We recommended adding this sentence to the new § 24.2-701.1(C). As the language of § 24.2-701.1(C) currently stands, a voter may vote an absentee ballot in the office of the general registrar or at a voting center approved by the electoral board. Until the second Saturday before an election, voters are required to fill out an application in order to vote absentee in-person. However, without language such as that quoted above added to the subsection, voters will not be permitted to apply for an absentee ballot in person at a voting center. The voter would need to apply at the office of the general registrar (where they could also vote absentee in-person), then travel to the voting center to cast a ballot there. Effectively, this renders any voting center open prior to the second Saturday preceding the election of no use. The General Assembly should add language similar to that above and also make clear that it applies to § 24.2-701.1.

Voting Centers

Currently, states have a number of different processes and mechanisms by which they allow localities to establish absentee "satellite offices", or what we have referred to as voting centers. For example, in North Carolina their locations are determined by the office of county board of elections[19]. While the county board has authority to choose these locations, they are subject to approval by the state board of elections and must be open during the same hours.[20] In Maryland, the absentee voting centers are established by the State Board of Elections in collaboration with local boards.[21] There, the number of voting centers depends on county population and ranges from one to five per county.[22]

[19] N.C.G.S.A §163A-1300 to §1631-1304
[20] Id.
[21] Maryland Election Law §10-301.1
[22] Id.

In Virginia, general registrars and local electoral board members have expressed concerns over the number of voting centers that will be necessary to successfully conduct no-excuse absentee voting. These groups have also expressed concerns over the need to fund any new or additional voting centers.

After reviewing the different state systems summarized on the National Conference of State Legislatures (NCSL) website and the concerns expressed by electoral boards and general registrars, we recommend the legislative changes summarized below.

The State Board of Elections maintains that localities themselves are in the best position to determine the number of new voting centers to accommodate in person absentee voting. However, we do recommend changes to the law regarding the establishment of voting centers.

We first recommend that voting centers be established, abolished, and/or changed by a locality's governing body. The Virginia Code already allows the governing body of each county, city, and town to establish polling places by ordinance.[23] The code also requires the governing body of each county, city, and town to provide funds to enable general registrars to maintain adequate facilities at each polling place.[24] We recommend applying those same requirements to the establishment of voting centers, so that governing bodies have the authority to establish those centers by ordinance, but so that they are also responsible for adequately funding those voting centers.

Another benefit of this process change, is that it would allow for public notice and input on voting centers changes, because they would be controlled by local ordinance. This change would also benefit localities, by giving them independent flexibility to increase, decrease, or move locations as necessary.

While we recommend making the process for establishing voting centers similar to the process to establishing polling places, we do recommend one difference in notice requirements. Typically, registrars must notify registered voters of a polling place change by mail at least fifteen days prior to the next general, special, or primary election.[25] This standard accounts for the fact that each registered voter has only one polling place on Election Day. By contrast, the no-excuse absentee voting law allows registered voters to vote absentee in person at any voting center in their locality. Therefore, we recommend that localities be required to post notice of a voting center change on the locality's website or publish the information in a newspaper of general circulation.[26] This standard will still provide voters with adequate notice of a change, while reducing the administrative and cost burden on general registrars.

Voting Hours for Voting Centers

Beginning with the November 3, 2020 General Election, Virginia's no-excuse absentee voting law requires voting centers to remain open for eight hours a day between 8 am and 5 pm.[27] To reduce voter confusion, we

[23] See Va. Code § 24.2-307.
[24] See Va. Code § 24.2-310
[25] See Va. Code § 24.2-306(B)
[26] The Virginia Code already uses this notice standard when there is a change in a locality's office of the general registrar. See Va. Code § 24.2-306(B).
[27] See Va. Code § 24.2-701.1(B)

recommend that the General Assembly pass legislation requiring uniformity in the hours that localities operate their voting centers. One option is for the General Assembly to allow localities to set their own absentee voting hours, with the requirement that all voting centers within the locality maintain the same voting hours. Another option is for the General Assembly to pass legislation setting uniform absentee voting hours for all voting centers in the Commonwealth.

Adoption of either of these plans will generate different sets of costs and logistical concerns. Requiring uniform hours across the Commonwealth would deprive localities of the flexibility to adapt to their individual needs and could make it difficult for localities to maintain staff at all voting centers throughout the absentee voting period. On the other hand, allowing localities to set their own hours could create voter confusion, especially in densely populated regions with large numbers of voters who move from one locality to another between election cycles.

Any discussion of requiring localities to open voting centers for specified hours should take into consideration two factors. One is the goal of providing access to the option of absentee voting to the greatest number of voters. In the absence of additional state funding, the other is the need for local registrars and directors of elections to work within the resources provided to them by their localities.

The General Assembly should also note that other states have had legal issues arise related to the hours in which they conduct in person absentee voting. For example, Texas' law allows for different voting locations to stay open for different amounts of hours on the same day.[28] In 2018, county leaders in Prairie View Texas scheduled fewer early-voting hours at voting centers near the A&M University campus than in whiter communities nearby.[29] As a consequence, the NAACP Legal Defense and Educational Fund led a number of students in filing a lawsuit against the county.

The Virginia Law provides significantly more stability and consistency in voting hours for those voting in person absentee. Specifically, the current law requires voting centers to remain open for eight hours a day between 8 am and 5 pm[30], whereas in Texas, some voting centers were open only three hours a day and others were open as many as twelve hours. However, as the legislature considers any changes to the current law, it should remain aware of potential civil rights issues that could come with significantly different voting hours in different areas. Requiring consistent hours within a locality would maintain uniformity and reduce the possibility of voter suppression.

Timeframe-Eligibility Expansion

The National Conference of State Legislatures (NCSL) website provides a number of facts and statistics about early voting throughout the United States. Of the thirty-nine states and the District of Columbia that allow for early voting (now including Virginia and Delaware), the average no-excuse absentee voting period is nineteen days in length and starts twenty-two days before Election Day. A number of states allow for no-excuse absentee

[28] See Tex. Elec. Code 85.001 and 85.002.

[29] The Washington Post Politics, "In rural Texas, black students' fight for voting access conjures a painful past." September 24, 2019. Retrieved from https://www.washingtonpost.com/politics/in-rural-texas-black-students-fight-for-voting-access-conjures-a-painful-past/2019/09/24/fa18e880-ca69-11e9-a1fe-ca46e8d573c0_story.html

[30] See Va. Code § 24.2-701.1(B)

voting for forty or more days before an election. These states include Maine, Michigan, Minnesota, New Jersey, South Dakota, Vermont, and Wyoming.[31]

As noted in this report's Executive Summary, Virginia has gradually expanded its pool of eligible absentee voters over the past several decades. These twelve-categories of excused absentee voters already account for a large number of registered voters in the Commonwealth of Virginia. Because so many Virginia voters are already eligible to vote in-person absentee, the inclusion of no-excuse absentee voting does not ~~drastically~~ significantly change the pool of individuals who may vote in-person before Election Day. Rather, the no-excuse period makes the administration of absentee voting more transparent and efficient by removing the task of categorizing voters into these categories through the submission of absentee ballot applications.

As the Commonwealth moves toward increasing voting choices for its registered voters, one option for Virginia is to eliminate excuse-based absentee voting and move toward allowing for a forty-five-day period of no excuse in person absentee voting.

There are a number of benefits that would come with extending no-excuse absentee voting to all forty-five days of absentee voting. First, allowing for all no-excuse absentee voting would reduce voter confusion. The current Virginia Absentee Ballot Application form lists twenty reasons that qualify a voter to vote using an absentee ballot. The absentee voting process as it stands to be enacted for the November 2020 General Election is bifurcated and will likely prove confusing to voters. When applying to vote absentee by mail, a voter must claim one of the twenty reasons. For the first thirty-five days of absentee voting, those who vote absentee in person are also required to claim one of the twenty reasons, whereas for the final seven days, voters need no reason to vote absentee in person.

As the law stands, an individual voting in person absentee on the seventh day before an election would not need to provide an excuse. By contrast, an individual voting absentee by mail during that period would have to provide one of the twenty excuses under 24.2-701. Providing for only no-excuse absentee voting would eliminate this double-standard.

If the legislature does not wish to extend no-excuse in person voting for the entire forty-five day absentee period, there are still benefits to extending the no-excuse period.[32] According to a report from American Progress, early voting can increase voter participation by two to four percent.[33] Additionally, eliminating early voting has been found to decrease turnout in communities of color.[34] In its 2014 report, the Bipartisan

[31] Colorado, Oregon, and Washington provide for all mail voting.

[32] See Center for American Progress's report "Increasing Voter Participation in America" by Danielle Root and Liz Kennedy (2018) available at https://www.americanprogress.org/issues/democracy/reports/2018/07/11/453319/increasing-voter-participation-america/

[33] Paul Gronke and others, "Convenience Voting," *Annual Review for Political Science* 11 (19) (2008): 437–455, available at http://earlyvoting.net/files/2012/05/Gronke2008-Convenience_Voting.pdf

[34] Vann R. Newkirk II, "What Early Voting in North Carolina Actually Reveals," *The Atlantic*, November 8, 2016, available at http://www.theatlantic.com/politics/archive/2016/11/north-carolina-early-voting/506963/

Presidential Commission on Election Administration recommended that states adopt early voting policies, in part to reduce long lines on Election Day.[35]

The average period of early voting is nineteen days. The average starting time for early voting is twenty-two days before an election. Additionally, early voting typically ends just a few days before Election Day. Further, of the states that allow early in-person voting, twenty-four and the District of Columbia allow for some weekend early voting. Specifically, twenty states plus the District of Columbia provide for Saturday voting. Additionally, five states allow for some Sunday voting.

Conclusion

The State Board of Elections and the Department of Elections are confident that Virginia will successfully implement the provisions of this Act and successfully conduct its first period of no excuse in person absentee voting. The Commonwealth has the benefit of learning from the thirty-nine states and the District of Columbia which already provide some form of in-person early voting. Further, Virginia has already added several acceptable absentee voting excuses over the past two decades. Registrars and Election Officials have experience adjusting to changes in absentee voting law, and should not find this change significantly more burdensome than previous changes to the law. To assist the General Assembly as well as the Virginia elections community, The State Board of Elections and Department of Elections are providing this table, summarizing the recommendations made throughout this report:

TABLE OF RECOMMENDATIONS

RECOMMENDATION	RELEVANT AUTHORITY
1) We recommend that the General Assembly consider legislation to adopt a common term for what is now referred to as "additional locations" under 24.2-701.1(C). As discussed in this report, colloquially these locations are also referred to as "satellite locations" or "voting centers."	Virginia Code § 24.2-701.1(C) and discussed in this report under *Voting Centers*, pages 5-6.
2) We recommend that general registrars and local election boards begin considering the need for voting centers/additional locations/satellite offices, to	Virginia Code § 24.2-701.1(C) and discussed in this report under *Voting Centers*, pages 5-6.

[35] 2014 report, the bipartisan Presidential Commission on Election Administration also recommended that states adopt early voting policies. Presidential Commission on Election Administration, "The American Voting Experience"; Lawrence Norden, "How to Fix Long Lines" (New York: Brennan Center for Justice, 2013).

accommodate increased absentee voter turnout in 2020.	
3) We recommend that general registrars prepare to recruit and train a sufficient number of officers of election for each voting center/additional location/satellite office. Under the code, "[A]t least two officers of election shall be present during all hours that absentee voting in person is available and shall represent the two major political parties…"	Virginia Code § 24.2-701.1(E) and discussed in this report under *Voting Centers*, pages 5-6.
4) We recommend that general registrars consider the needs of each voting center/additional location/satellite office, including the need for physical space, parking spaces, equipment (including tabulators), and poll books.	Virginia Code § 24.2-701.1(C) and discussed in this report under *Voting Centers*, pages 5-6.
5) We recommend that the General Assembly adopt the proposed technical changes bill, which is summarized in the chart on page 7 of this report.	Amends Virginia Code § 24.2-701.1(A),(C) and discussed in this report under *Technical Changes*, page 8.
6) We recommend that the General Assembly adopt the proposed voting centers bill, which is summarized in the chart on page 7 of this report.	Amends Virginia Code § 24.2-701.1(B)-(F) and adds Virginia Code 24.2-701.2. This topic is discussed in this report under *Voting Centers*, pages 8-9.
7) We recommend that the General Assembly consider an amendment to current law that either requires the voting centers/additional locations/satellite offices within a locality to maintain the same hours of operation during the absentee voting period, or requires uniform voting hours for all voting centers/additional locations/satellite offices within the Commonwealth of Virginia.	Virginia Code § 24.2-701.1(B) and discussed in this report under *Voting Hours for Voting Centers*, pages 9-10.
8) We recommend that the General Assembly adopt the proposed timeframe eligibility bill, which would extend the no-excuse absentee voting period to the full forty-five day period of absentee voting.	Virginia Code § 24.2-701.1(A) and discussed in this report under *Timeframe Eligibility Expansion*, pages 10-11.

Respectfully Submitted by the State Board of Elections:

____

Robert H. Brink, Chairman

____

John O’Bannon, Vice Chair

____

Jamilah D. LeCruise, Secretary

★ VIRGINIA ★
STATE BOARD of ELECTIONS

Stand by Your Ad

BOARD WORKING PAPERS
Arielle A. Schneider
Policy Analyst

★ VIRGINIA ★

DEPARTMENT *of* ELECTIONS

Stand By Your Ad

November 18, 2019

State Board of Elections Meeting

Print Media

1.	Arika Phillips For CCPS School Board	CC-19-00127
2.	Charon Coffee Price	
3.	Darby McGeorge	
4.	Darryl V. Parker	
5.	Friends of Andrew Cullip Campaign	CC-19-00912
6.	Friends of Chris Peace	CC-12-00165
7.	Friends of David Hardin	CC-19-00532
8.	Friends of Joe Dombroski	CC-19-01133

Print Media (cont.)

9. Friends of Paul Petrauskas	CC-19-00793
10. Friends of Scott Mayausky	CC-13-00569
11. Friends of Tim McLaughlin	CC-15-00154
12. Friends of Virginia	CC-19-00343
13. Friends of Will Gardner	CC-19-00541
14. Gerald Mitchell for Sheriff	CC-19-00884
15. Gilbert A. Smith	
16. John Edward Hall	

Print Media (cont.)

17. Kiser for Delegate	CC-19-00739
18. Lyndsey Dotterer	
19. Michael J. Hallahan, II - Candidate for Supervisor	CC-19-00259
20. Missy for Senate	CC-18-00546
21. Partnership for New Kent 2030 Political Action Committee	PAC-19-01032
22. Ralph Parham for Treasurer	CC-19-00199
23. Reginald A. Williams, Sr.	
24. Samantha Bohannon, Candidate	CC-19-01091

Print Media (cont.)

25. Shick for Gainesboro District School Board	CC-19-00724
26. Stop Trafficking Augusta	PAC-19-01040
27. Sue Kass for School Board	CC-19-00933
28. Wade for Sheriff.	CC-19-00844
29. Whitbeck for Chairman	CC-19-00174
30. Winchester-Frederick Democratic Committee	

Advertisement, 24.2-955.1

“*Advertisement* means any message appearing in the print media, on television, or on radio that constitutes a contribution or expenditure under Chapter 9.3”

Contribution or Expenditure, 24.2-945.1

“*Contribution* means money and services of any amount, in-kind contribution, and any other thing of value, given, advanced, loaned, or in any other way provided to a candidate, campaign committee, political committee, or person for the purpose of expressly advocating the election or defeat of a clearly identified candidate … Contribution includes money, services, or things of value in any way provided by a candidate to his own campaign …”

“*Expenditure* means money and services of any amount, and any other thing of value, paid, loaned, provided or in any other way disbursed by any candidate, campaign committee, political committee, or person for the purpose of expressly advocating the election or defeat of a clearly identified candidate …”

Candidate, 24.2-101

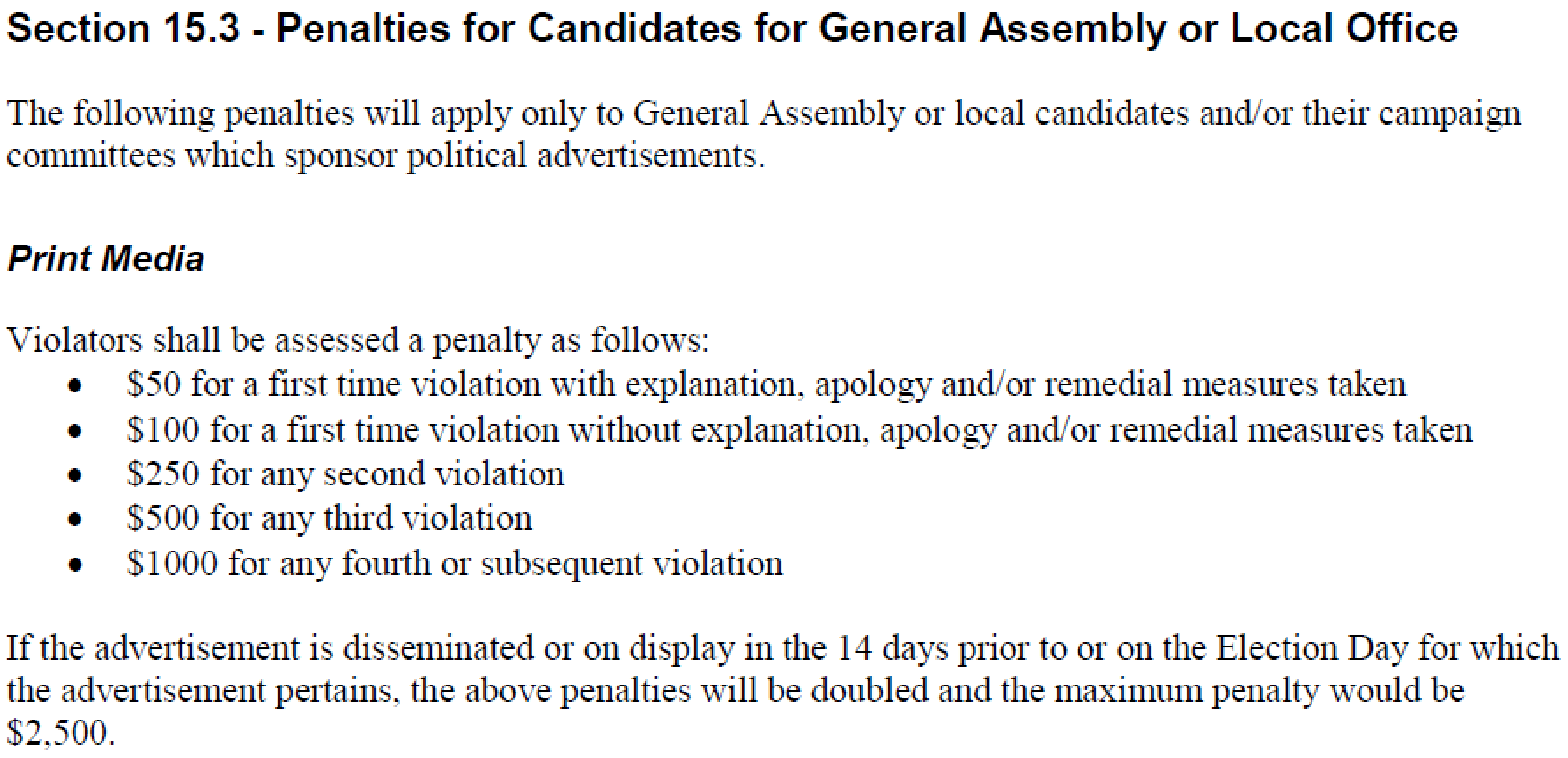
“*Candidate* means a person who seeks or campaigns for an office of the Commonwealth or one of its governmental units in a general, primary, or special election and who is qualified to have his name placed on the ballot. …

For the purposes of Chapters 9.3 and 9.5, “candidate” shall include any person who raises or spends funds in order to seek or campaign for an office of the Commonwealth, excluding federal offices, or one of its governmental units in a party nomination process or general, primary, or special election; and such person shall be considered a candidate until a final report is filed pursuant to Article 8 of Chapter 9.3.”

Express Advocacy

Express Advocacy – A direct or indirect contribution, in-kind contribution, independent expenditure or loan made to a candidate or political committee for the purpose of influencing the outcome of an election; *an advertisement that refers to a party or candidate(s) by name and states "Vote for…"; "Support"; "Elect…"; "Smith for Congress"; "Send Him Home"; "Oppose", etc.*

Schedule of Penalties *candidates for General Assembly or local candidates*



Section 15.3 - Penalties for Candidates for General Assembly or Local Office

The following penalties will apply only to General Assembly or local candidates and/or their campaign committees which sponsor political advertisements.

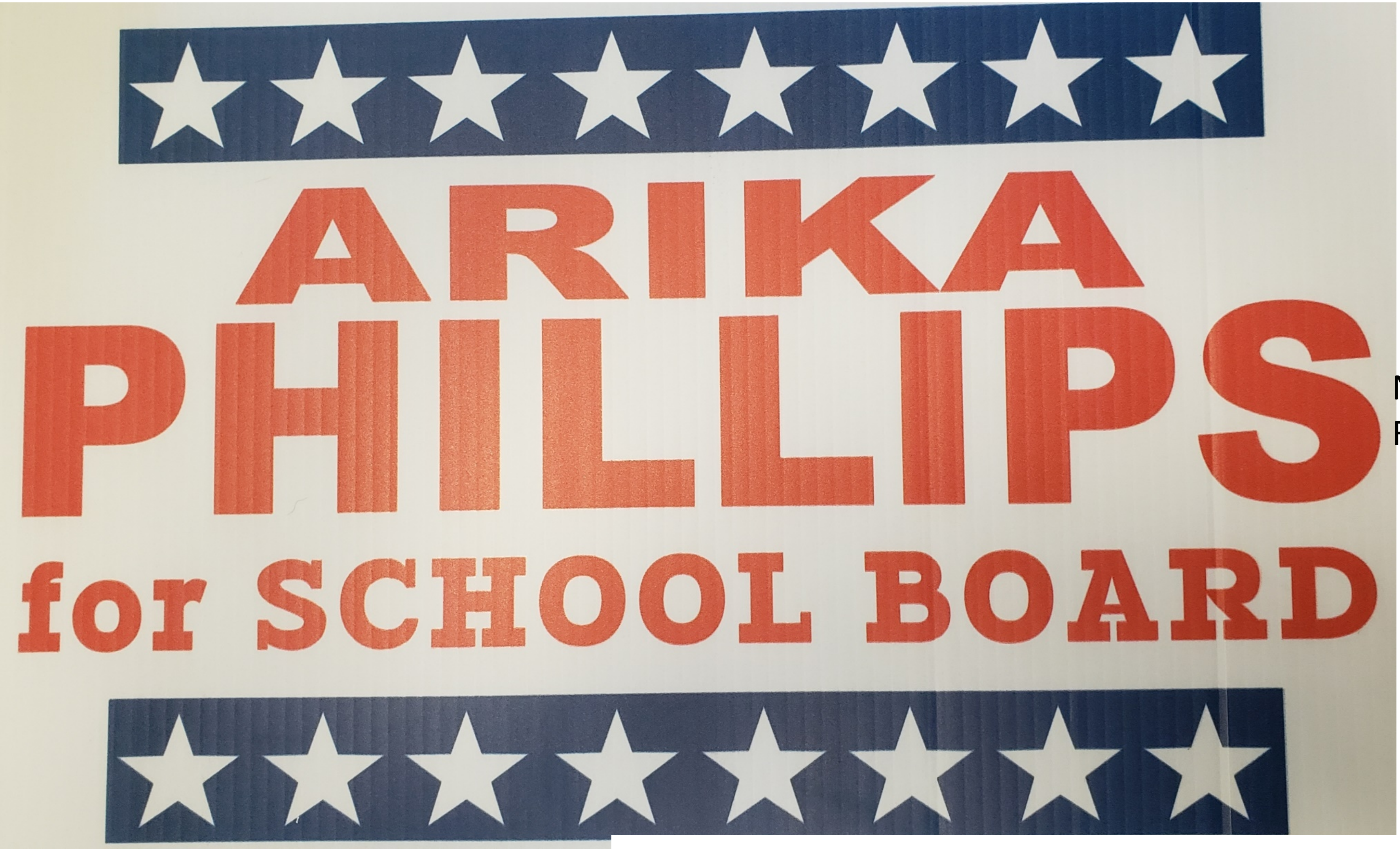
Print Media

Violators shall be assessed a penalty as follows:

- $50 for a first time violation with explanation, apology and/or remedial measures taken
- $100 for a first time violation without explanation, apology and/or remedial measures taken
- $250 for any second violation
- $500 for any third violation
- $1000 for any fourth or subsequent violation

If the advertisement is disseminated or on display in the 14 days prior to or on the Election Day for which the advertisement pertains, the above penalties will be doubled and the maximum penalty would be $2,500.

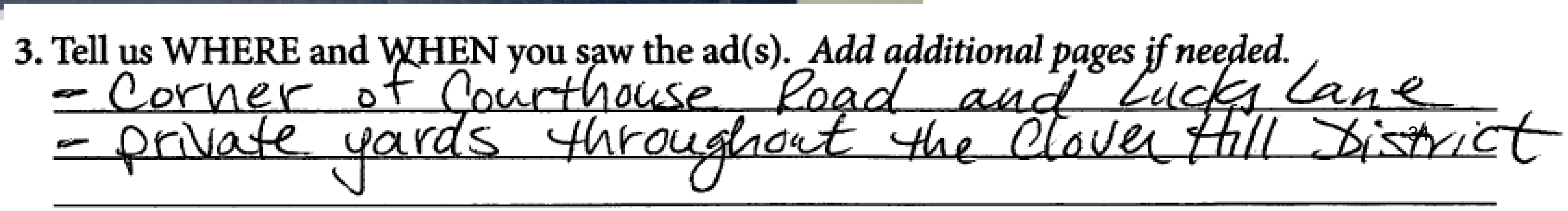
1. Arika Phillips for CCPS School Board CC-19-00127



Anonymous Complaint sent via USPS

One (1) Actual Sign

No violation date listed on complaint
Received by ELECT 10/24/2019



3. Tell us WHERE and WHEN you saw the ad(s). *Add additional pages if needed.*

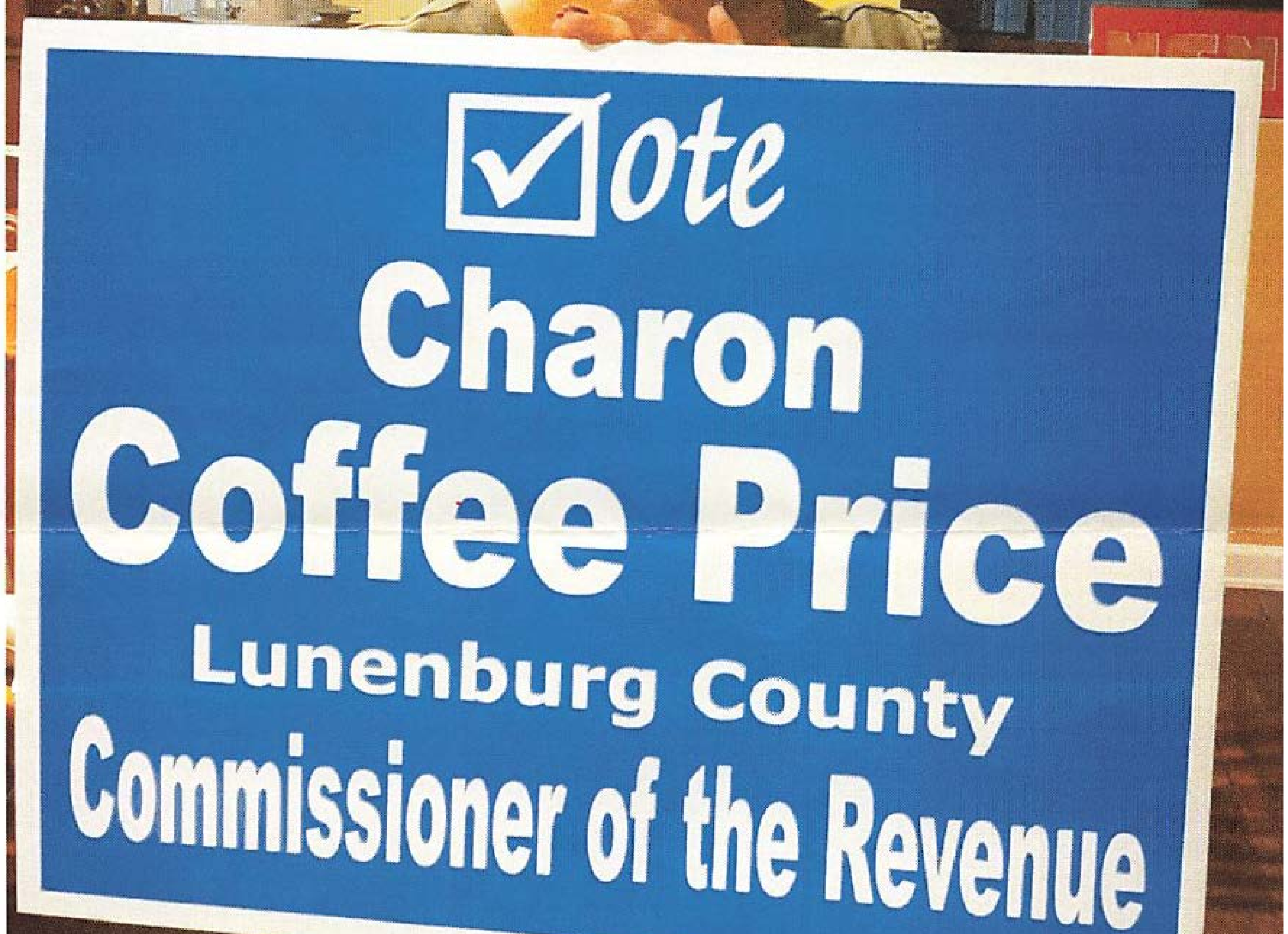
- Corner of Courthouse Road and Lucks Lane
- private yards throughout the Clover Hill District

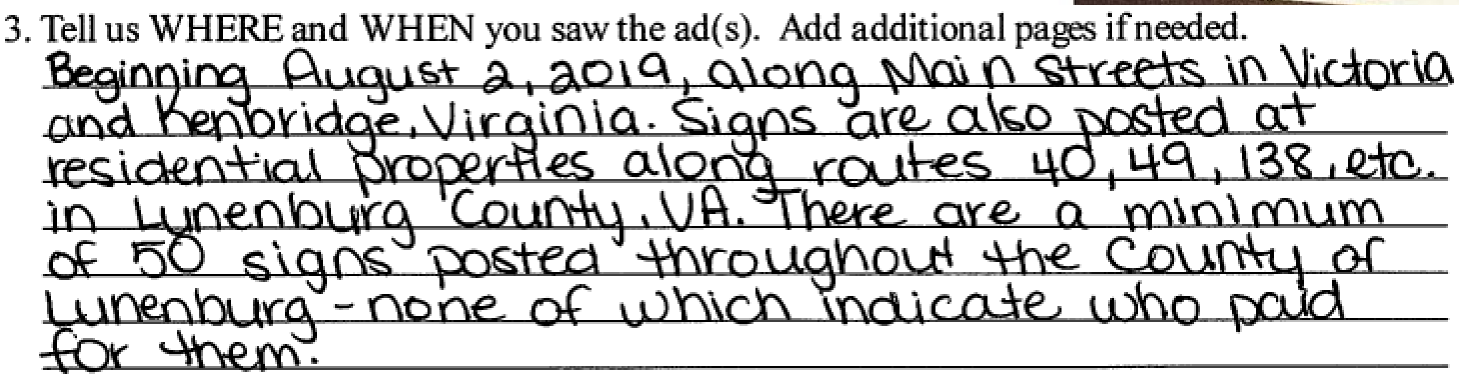
2.Charon Coffee Price

One sign

Anonymous via Snail mail

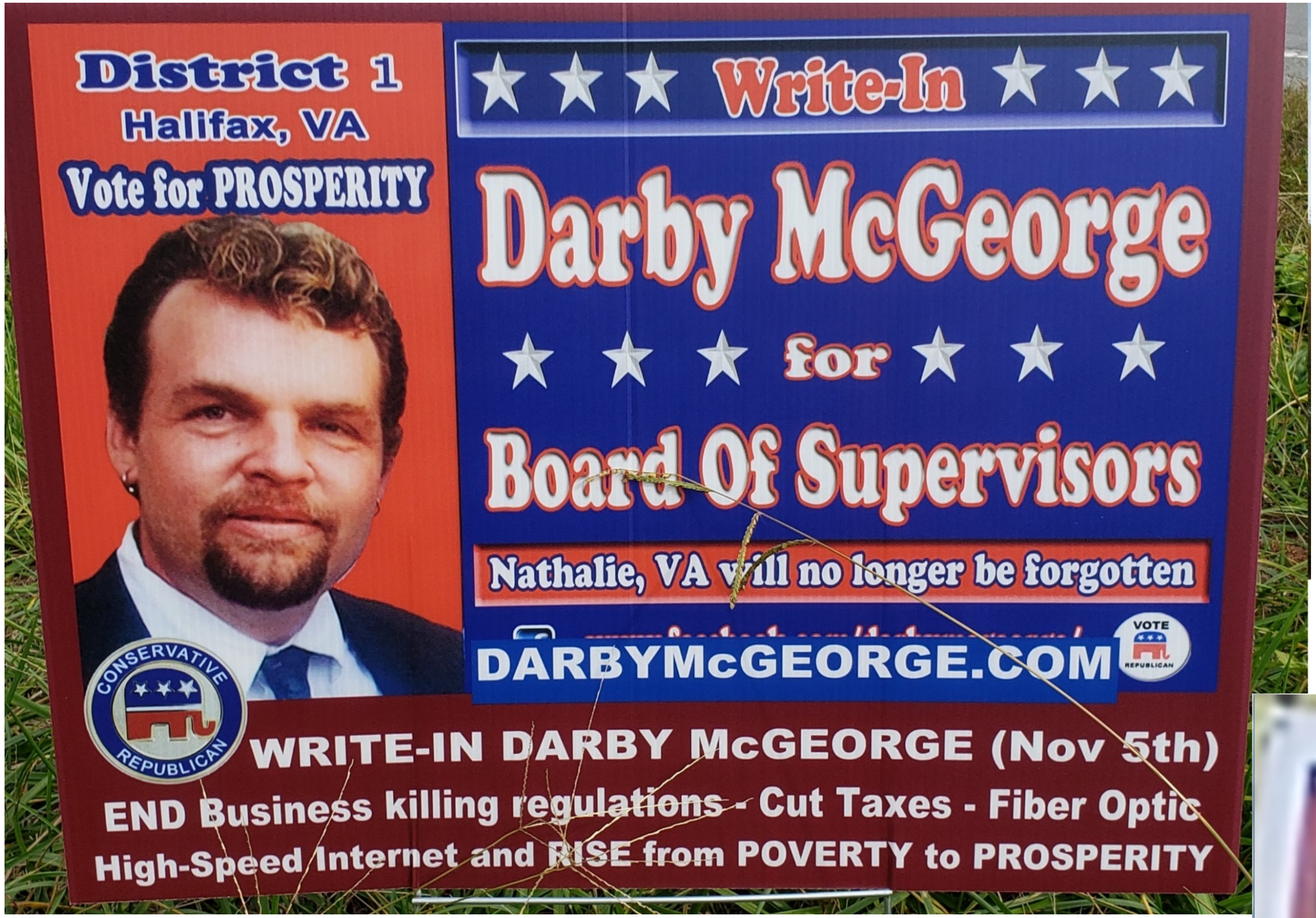
Violation Date August 2, 2019




3. Tell us WHERE and WHEN you saw the ad(s). Add additional pages if needed.

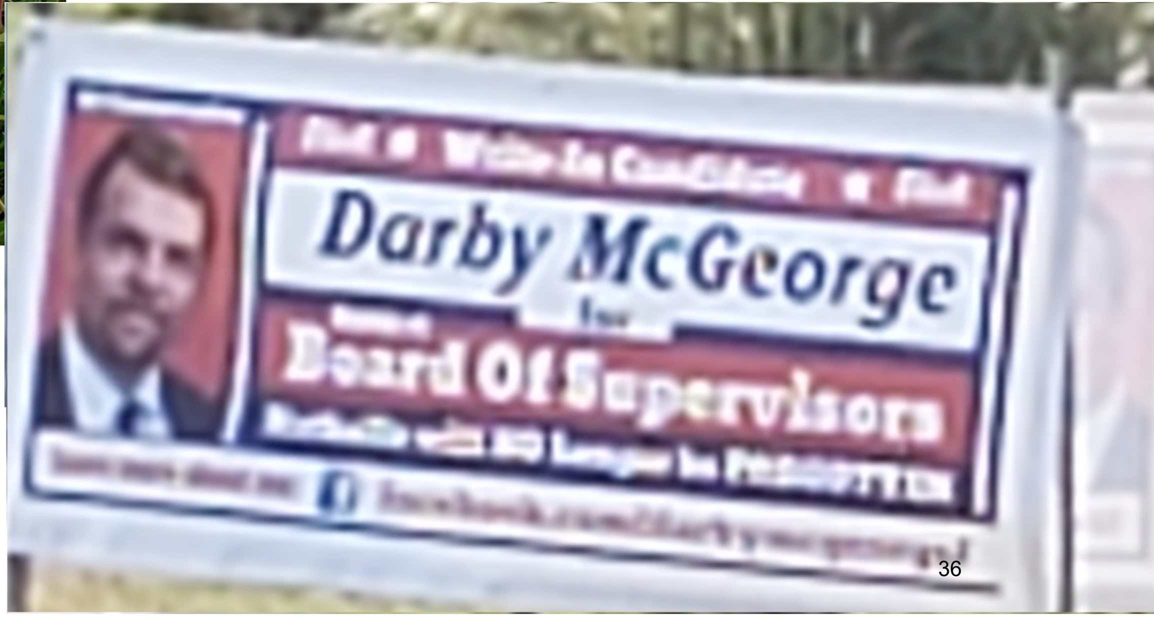
Beginning August 2, 2019, along Main streets in Victoria
and Kenbridge, Virginia. Signs are also posted at
residential properties along routes 40, 49, 138, etc.
in Lunenburg County, VA. There are a minimum
of 50 signs posted throughout the County of
Lunenburg - none of which indicate who paid
for them.

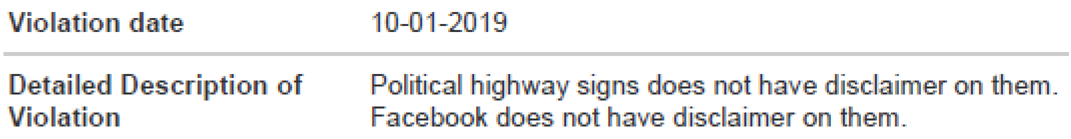
3. Darby McGeorge


District 1
Halifax, VA
Vote for PROSPERITY
Write-In
Darby McGeorge
for
Board Of Supervisors
Nathalie, VA will no longer be forgotten
DARBYMcGEORGE.COM
VOTE
REPUBLICAN
CONSERVATIVE
REPUBLICAN
WRITE-IN DARBY McGEORGE (Nov 5th)
END Business killing regulations - Cut Taxes - Fiber Optic
High-Speed Internet and RISE from POVERTY to PROSPERITY

Two signs

Online Complaint by Calvin R. Short





Violation date	10-01-2019
Detailed Description of Violation	Political highway signs does not have disclaimer on them. Facebook does not have disclaimer on them.

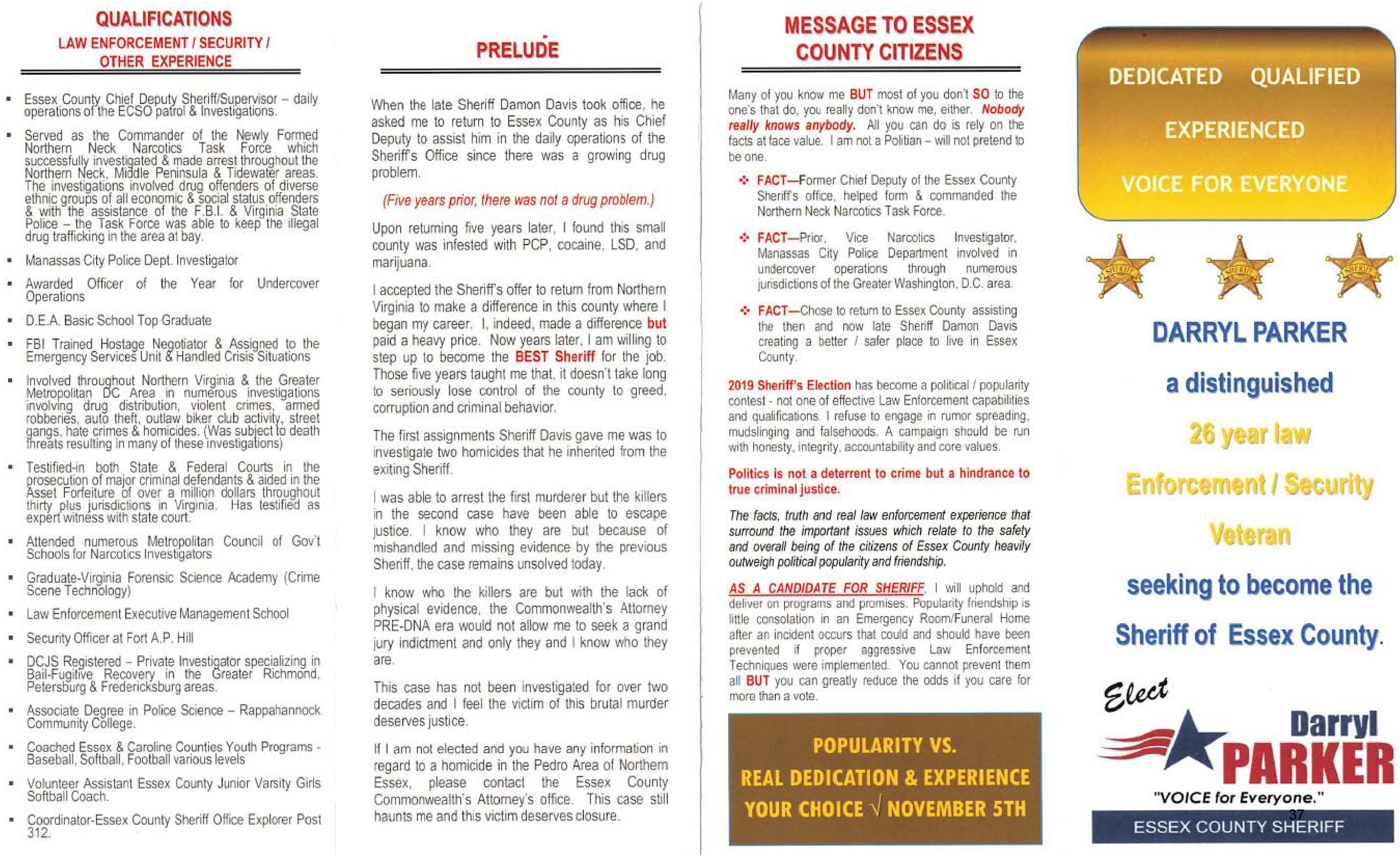
4. Darryl V. Parker

Front page of Pamphlet – Darryl Parker

One pamphlet

Anonymous – snail mail

Violation date Sept. 25, 2019



QUALIFICATIONS

LAW ENFORCEMENT / SECURITY / OTHER EXPERIENCE

- Essex County Chief Deputy Sheriff/Supervisor – daily operations of the ECSO patrol & Investigations.
- Served as the Commander of the Newly Formed Northern Neck Narcotics Task Force which successfully investigated & made arrest throughout the Northern Neck, Middle Peninsula & Tidewater areas. The investigations involved drug offenders of diverse ethnic groups of all economic & social status offenders & with the assistance of the F.B.I. & Virginia State Police – the Task Force was able to keep the illegal drug trafficking in the area at bay.
- Manassas City Police Dept. Investigator
- Awarded Officer of the Year for Undercover Operations
- D.E.A. Basic School Top Graduate
- FBI Trained Hostage Negotiator & Assigned to the Emergency Services Unit & Handled Crisis Situations
- Involved throughout Northern Virginia & the Greater Metropolitan DC Area in numerous investigations involving drug distribution, violent crimes, armed robberies, auto theft, outlaw biker club activity, street gangs, hate crimes & homicides. (Was subject to death threats resulting in many of these investigations)
- Testified-in both State & Federal Courts in the prosecution of major criminal defendants & aided in the Asset Forfeiture of over a million dollars throughout thirty plus jurisdictions in Virginia. Has testified as expert witness with state court.
- Attended numerous Metropolitan Council of Gov't Schools for Narcotics Investigators
- Graduate-Virginia Forensic Science Academy (Crime Scene Technology)
- Law Enforcement Executive Management School
- Security Officer at Fort A.P. Hill
- DCJS Registered – Private Investigator specializing in Bail-Fugitive Recovery in the Greater Richmond, Petersburg & Fredericksburg areas.
- Associate Degree in Police Science – Rappahannock Community College.
- Coached Essex & Caroline Counties Youth Programs - Baseball, Softball, Football various levels
- Volunteer Assistant Essex County Junior Varsity Girls Softball Coach.
- Coordinator-Essex County Sheriff Office Explorer Post 312.

PRELUDE

When the late Sheriff Damon Davis took office, he asked me to return to Essex County as his Chief Deputy to assist him in the daily operations of the Sheriff's Office since there was a growing drug problem.

(Five years prior, there was not a drug problem.)

Upon returning five years later, I found this small county was infested with PCP, cocaine, LSD, and marijuana.

I accepted the Sheriff's offer to return from Northern Virginia to make a difference in this county where I began my career. I, indeed, made a difference **but** paid a heavy price. Now years later, I am willing to step up to become the **BEST Sheriff** for the job. Those five years taught me that, it doesn't take long to seriously lose control of the county to greed, corruption and criminal behavior.

The first assignments Sheriff Davis gave me was to investigate two homicides that he inherited from the exiting Sheriff.

I was able to arrest the first murderer but the killers in the second case have been able to escape justice. I know who they are but because of mishandled and missing evidence by the previous Sheriff, the case remains unsolved today.

I know who the killers are but with the lack of physical evidence, the Commonwealth's Attorney PRE-DNA era would not allow me to seek a grand jury indictment and only they and I know who they are.

This case has not been investigated for over two decades and I feel the victim of this brutal murder deserves justice.

If I am not elected and you have any information in regard to a homicide in the Pedro Area of Northern Essex, please contact the Essex County Commonwealth's Attorney's office. This case still haunts me and this victim deserves closure.

MESSAGE TO ESSEX COUNTY CITIZENS

Many of you know me **BUT** most of you don't **SO** to the one's that do, you really don't know me, either. ***Nobody really knows anybody.*** All you can do is rely on the facts at face value. I am not a Politian – will not pretend to be one.

- **FACT—**Former Chief Deputy of the Essex County Sheriff's office, helped form & commanded the Northern Neck Narcotics Task Force.
- **FACT—**Prior, Vice Narcotics Investigator, Manassas City Police Department involved in undercover operations through numerous jurisdictions of the Greater Washington, D.C. area.
- **FACT—**Chose to return to Essex County assisting the then and now late Sheriff Damon Davis creating a better / safer place to live in Essex County.

2019 Sheriff's Election has become a political / popularity contest - not one of effective Law Enforcement capabilities and qualifications. I refuse to engage in rumor spreading, mudslinging and falsehoods. A campaign should be run with honesty, integrity, accountability and core values.

Politics is not a deterrent to crime but a hindrance to true criminal justice.

The facts, truth and real law enforcement experience that surround the important issues which relate to the safety and overall being of the citizens of Essex County heavily outweigh political popularity and friendship.

AS A CANDIDATE FOR SHERIFF, I will uphold and deliver on programs and promises. Popularity friendship is little consolation in an Emergency Room/Funeral Home after an incident occurs that could and should have been prevented if proper aggressive Law Enforcement Techniques were implemented. You cannot prevent them all **BUT** you can greatly reduce the odds if you care for more than a vote.

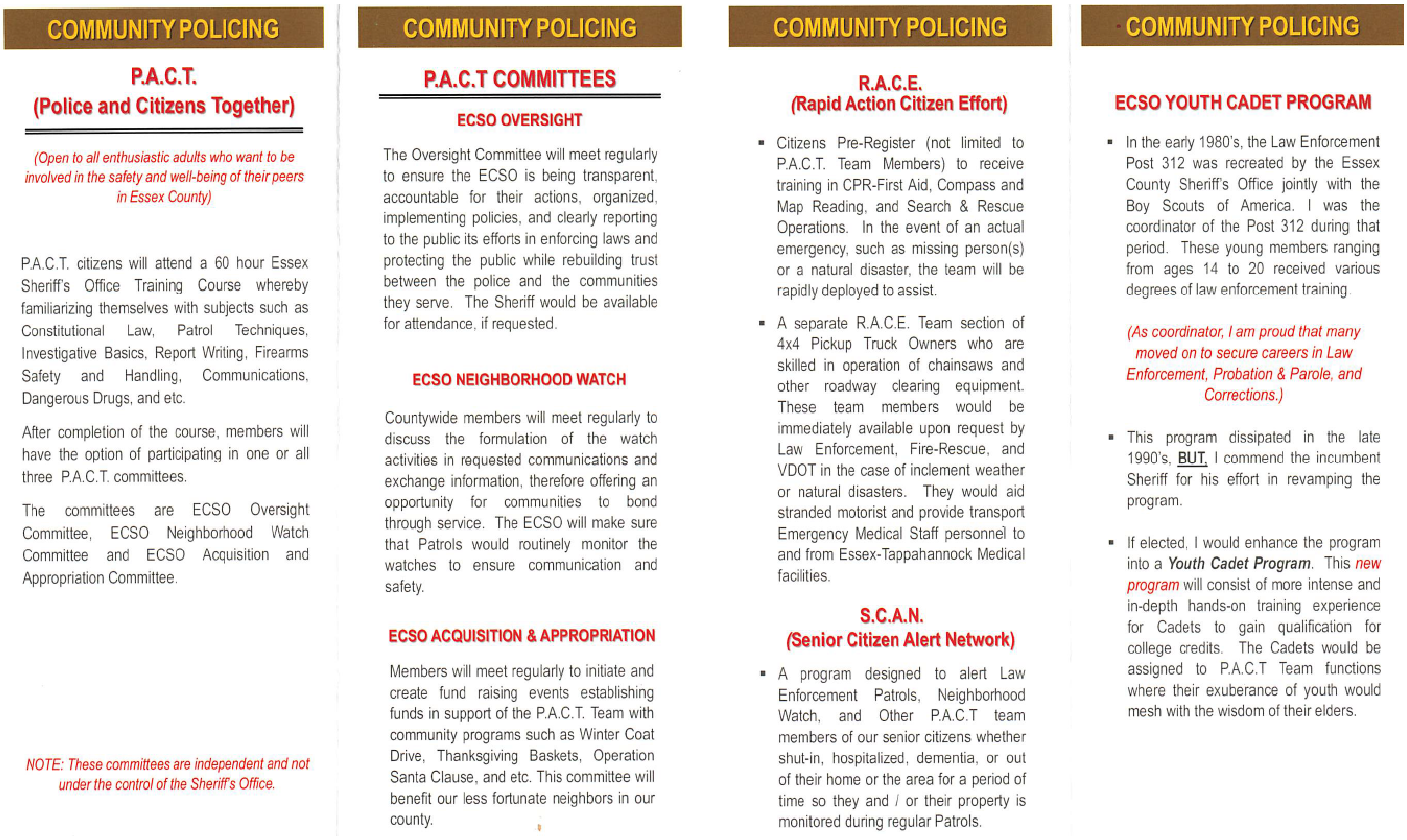
POPULARITY VS.
REAL DEDICATION & EXPERIENCE
YOUR CHOICE √ NOVEMBER 5TH

DEDICATED QUALIFIED
EXPERIENCED
VOICE FOR EVERYONE

DARRYL PARKER
a distinguished
26 year law
Enforcement / Security
Veteran
seeking to become the
Sheriff of Essex County.

Elect
Darryl PARKER
"VOICE for Everyone."
ESSEX COUNTY SHERIFF

Back Page of Pamphlet - Darryl Parker



COMMUNITY POLICING

P.A.C.T. (Police and Citizens Together)

(Open to all enthusiastic adults who want to be involved in the safety and well-being of their peers in Essex County)

P.A.C.T. citizens will attend a 60 hour Essex Sheriff's Office Training Course whereby familiarizing themselves with subjects such as Constitutional Law, Patrol Techniques, Investigative Basics, Report Writing, Firearms Safety and Handling, Communications, Dangerous Drugs, and etc.

After completion of the course, members will have the option of participating in one or all three P.A.C.T. committees.

The committees are ECSO Oversight Committee, ECSO Neighborhood Watch Committee and ECSO Acquisition and Appropriation Committee.

NOTE: These committees are independent and not under the control of the Sheriff's Office.

COMMUNITY POLICING

P.A.C.T COMMITTEES

ECSO OVERSIGHT

The Oversight Committee will meet regularly to ensure the ECSO is being transparent, accountable for their actions, organized, implementing policies, and clearly reporting to the public its efforts in enforcing laws and protecting the public while rebuilding trust between the police and the communities they serve. The Sheriff would be available for attendance, if requested.

ECSO NEIGHBORHOOD WATCH

Countywide members will meet regularly to discuss the formulation of the watch activities in requested communications and exchange information, therefore offering an opportunity for communities to bond through service. The ECSO will make sure that Patrols would routinely monitor the watches to ensure communication and safety.

ECSO ACQUISITION & APPROPRIATION

Members will meet regularly to initiate and create fund raising events establishing funds in support of the P.A.C.T. Team with community programs such as Winter Coat Drive, Thanksgiving Baskets, Operation Santa Clause, and etc. This committee will benefit our less fortunate neighbors in our county.

COMMUNITY POLICING

R.A.C.E. (Rapid Action Citizen Effort)

- Citizens Pre-Register (not limited to P.A.C.T. Team Members) to receive training in CPR-First Aid, Compass and Map Reading, and Search & Rescue Operations. In the event of an actual emergency, such as missing person(s) or a natural disaster, the team will be rapidly deployed to assist.
- A separate R.A.C.E. Team section of 4x4 Pickup Truck Owners who are skilled in operation of chainsaws and other roadway clearing equipment. These team members would be immediately available upon request by Law Enforcement, Fire-Rescue, and VDOT in the case of inclement weather or natural disasters. They would aid stranded motorist and provide transport Emergency Medical Staff personnel to and from Essex-Tappahannock Medical facilities.

S.C.A.N. (Senior Citizen Alert Network)

- A program designed to alert Law Enforcement Patrols, Neighborhood Watch, and Other P.A.C.T team members of our senior citizens whether shut-in, hospitalized, dementia, or out of their home or the area for a period of time so they and / or their property is monitored during regular Patrols.

COMMUNITY POLICING

ECSO YOUTH CADET PROGRAM

- In the early 1980's, the Law Enforcement Post 312 was recreated by the Essex County Sheriff's Office jointly with the Boy Scouts of America. I was the coordinator of the Post 312 during that period. These young members ranging from ages 14 to 20 received various degrees of law enforcement training.

(As coordinator, I am proud that many moved on to secure careers in Law Enforcement, Probation & Parole, and Corrections.)

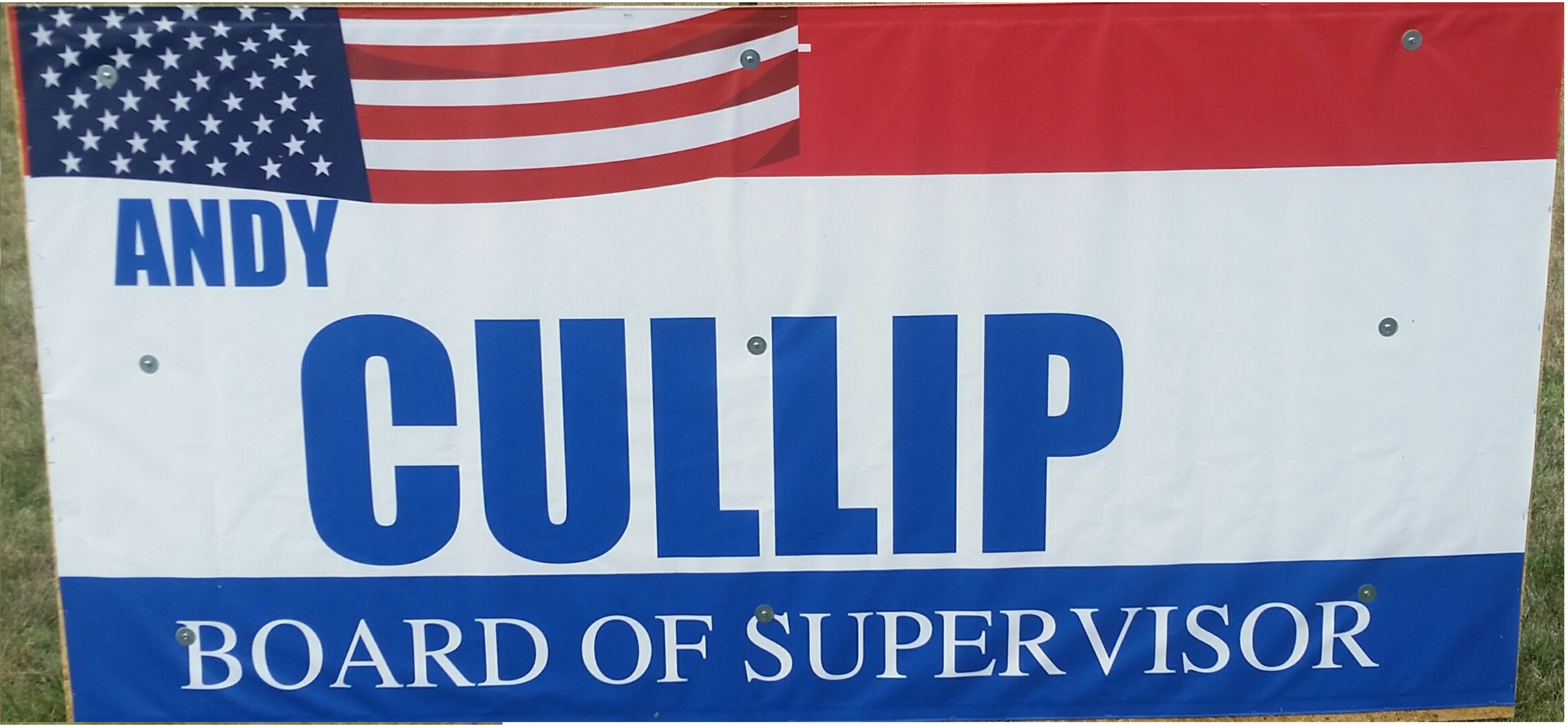
- This program dissipated in the late 1990's, **BUT,** I commend the incumbent Sheriff for his effort in revamping the program.
- If elected, I would enhance the program into a ***Youth Cadet Program***. This new program will consist of more intense and in-depth hands-on training experience for Cadets to gain qualification for college credits. The Cadets would be assigned to P.A.C.T Team functions where their exuberance of youth would mesh with the wisdom of their elders.

5. Friends of Andrew Cullip CC-19-00912

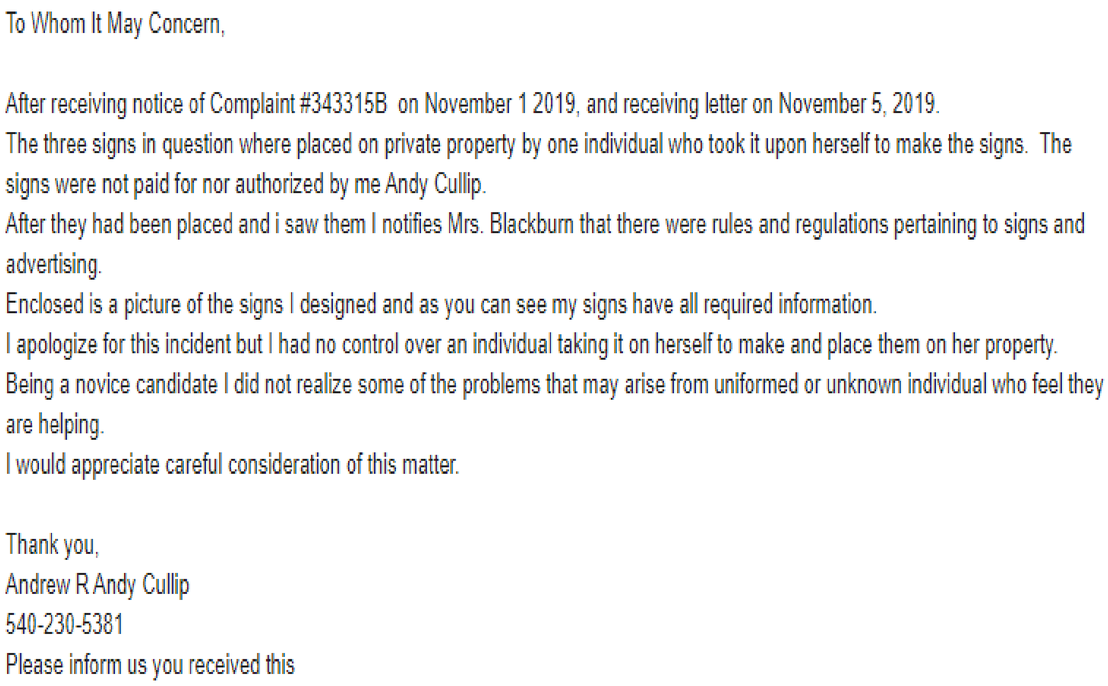
Large Banner attached to pressboard

Violation date	09-23-2019

No disclosure complaint filed online by Joseph Guthrie



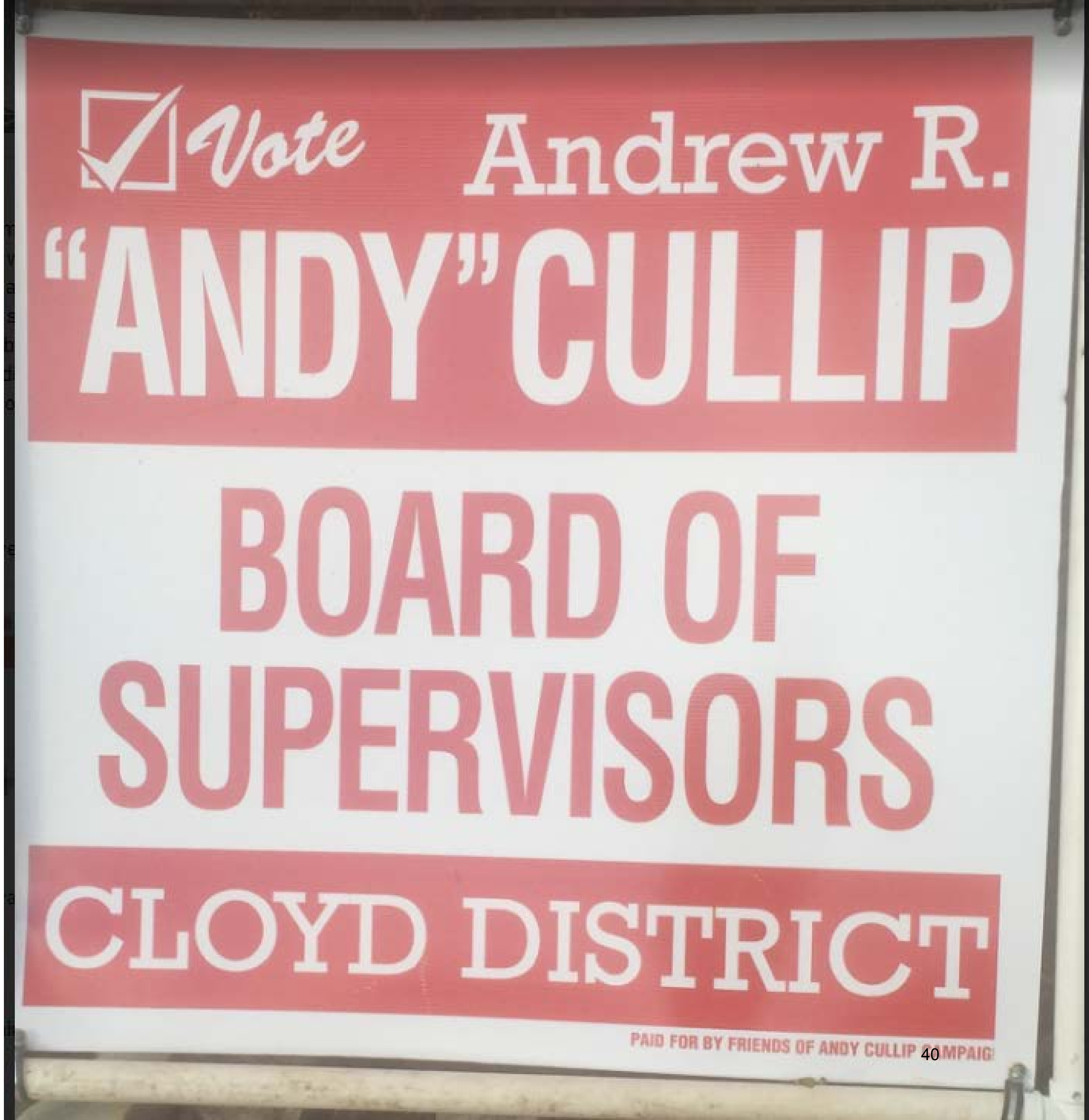
Cullip Response



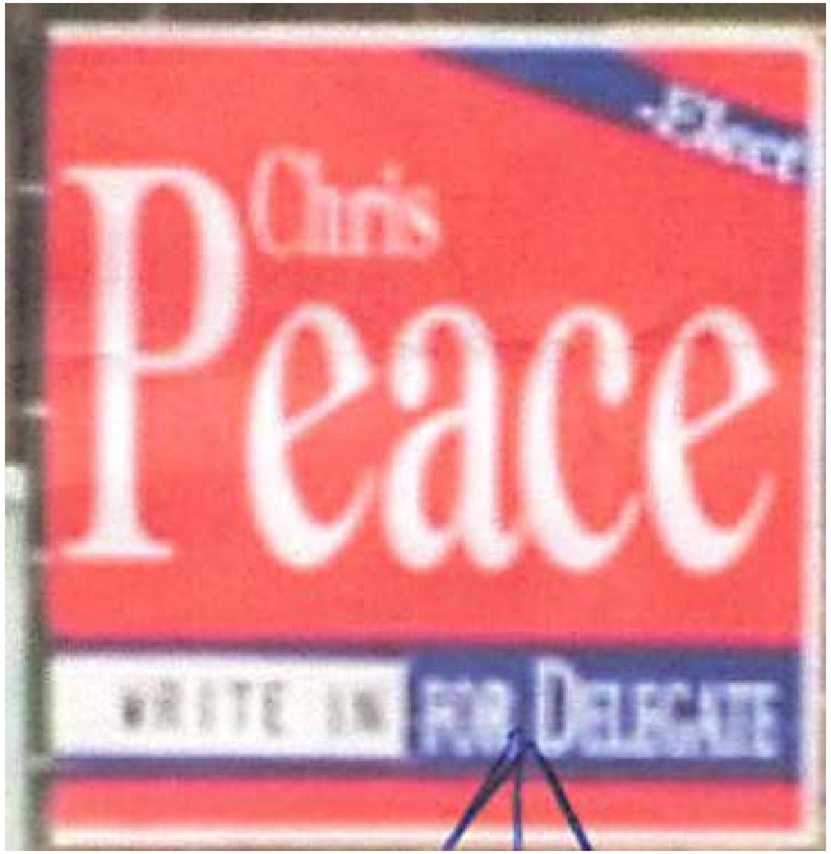
To Whom It May Concern,

After receiving notice of Complaint #343315B on November 1 2019, and receiving letter on November 5, 2019.
The three signs in question where placed on private property by one individual who took it upon herself to make the signs. The signs were not paid for nor authorized by me Andy Cullip.
After they had been placed and i saw them I notifies Mrs. Blackburn that there were rules and regulations pertaining to signs and advertising.
Enclosed is a picture of the signs I designed and as you can see my signs have all required information.
I apologize for this incident but I had no control over an individual taking it on herself to make and place them on her property.
Being a novice candidate I did not realize some of the problems that may arise from uniformed or unknown individual who feel they are helping.
I would appreciate careful consideration of this matter.

Thank you,
Andrew R Andy Cullip
540-230-5381
Please inform us you received this



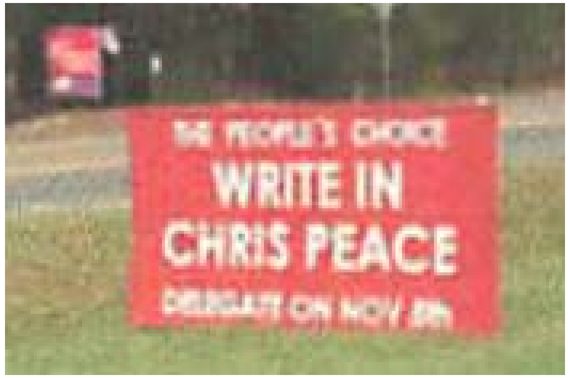
6. Friends of Chris Peace CC-12-00165

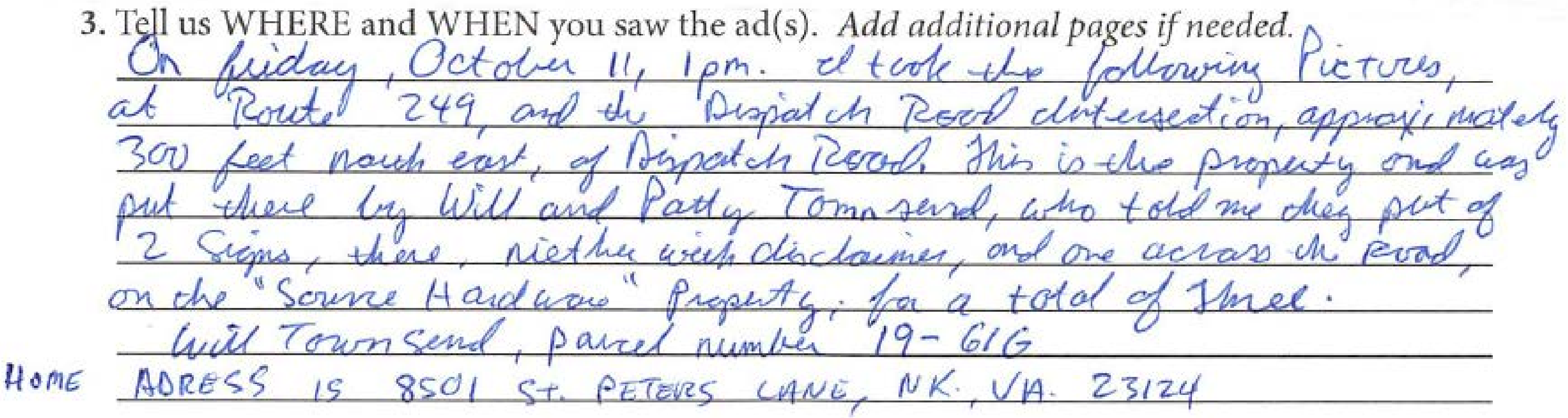


3 signs

Anonymous complaint received via snail mail

Violation Date October 11, 2019

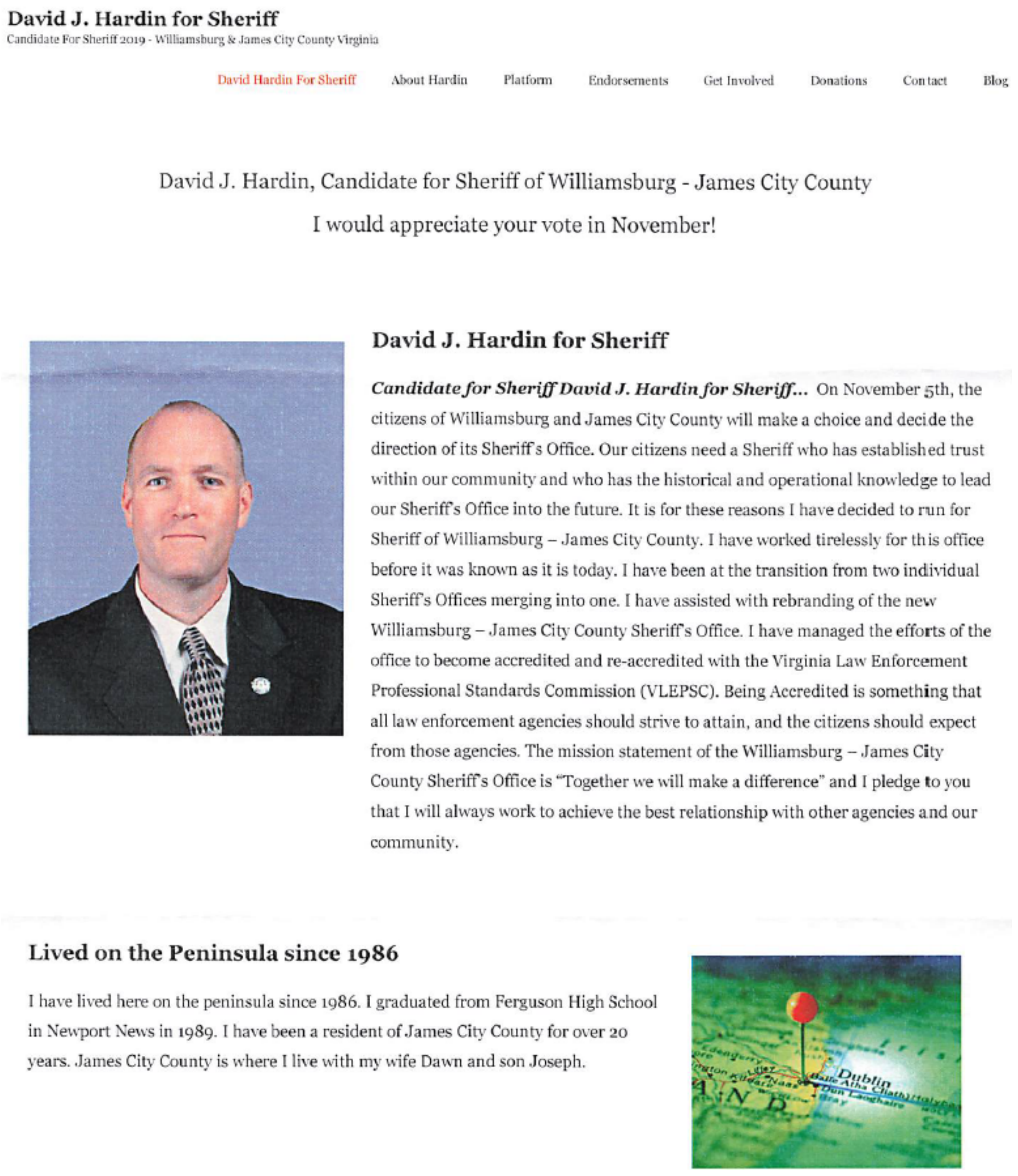




3. Tell us WHERE and WHEN you saw the ad(s). *Add additional pages if needed.*

On friday, October 11, 1pm. I took the following Pictures,
at Route 249, and the Dispatch Road intersection, approximately
300 feet north east, of Dispatch Road. This is the property and was
put there by Will and Patty Townsend, who told me they put of
2 Signs, there, niether with disclaimer, and one across the road,
on the "Source Hardware" property; for a total of Three.
Will Townsend, parcel number 19-61G
HOME ADRESS IS 8501 ST. PETERS LANE, NK., VA. 23124

7. Friends of David Hardin CC-19-00532



David J. Hardin for Sheriff
Candidate For Sheriff 2019 - Williamsburg & James City County Virginia

David J. Hardin, Candidate for Sheriff of Williamsburg - James City County

I would appreciate your vote in November!

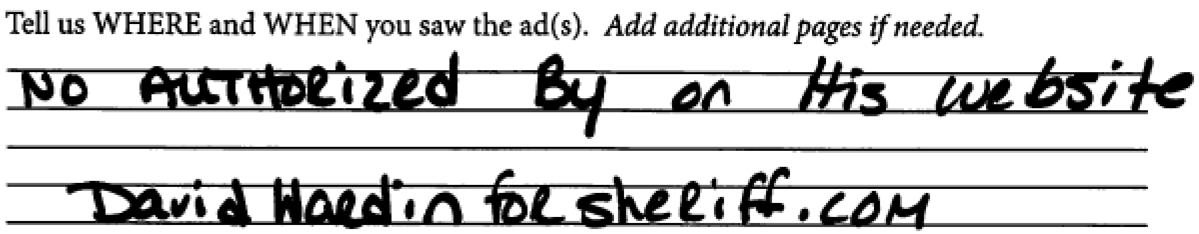
David J. Hardin for Sheriff

Candidate for Sheriff David J. Hardin for Sheriff… On November 5th, the citizens of Williamsburg and James City County will make a choice and decide the direction of its Sheriff's Office. Our citizens need a Sheriff who has established trust within our community and who has the historical and operational knowledge to lead our Sheriff's Office into the future. It is for these reasons I have decided to run for Sheriff of Williamsburg – James City County. I have worked tirelessly for this office before it was known as it is today. I have been at the transition from two individual Sheriff's Offices merging into one. I have assisted with rebranding of the new Williamsburg – James City County Sheriff's Office. I have managed the efforts of the office to become accredited and re-accredited with the Virginia Law Enforcement Professional Standards Commission (VLEPSC). Being Accredited is something that all law enforcement agencies should strive to attain, and the citizens should expect from those agencies. The mission statement of the Williamsburg – James City County Sheriff's Office is "Together we will make a difference" and I pledge to you that I will always work to achieve the best relationship with other agencies and our community.

Lived on the Peninsula since 1986

I have lived here on the peninsula since 1986. I graduated from Ferguson High School in Newport News in 1989. I have been a resident of James City County for over 20 years. James City County is where I live with my wife Dawn and son Joseph.

Anonymous complaint sent via snail mail

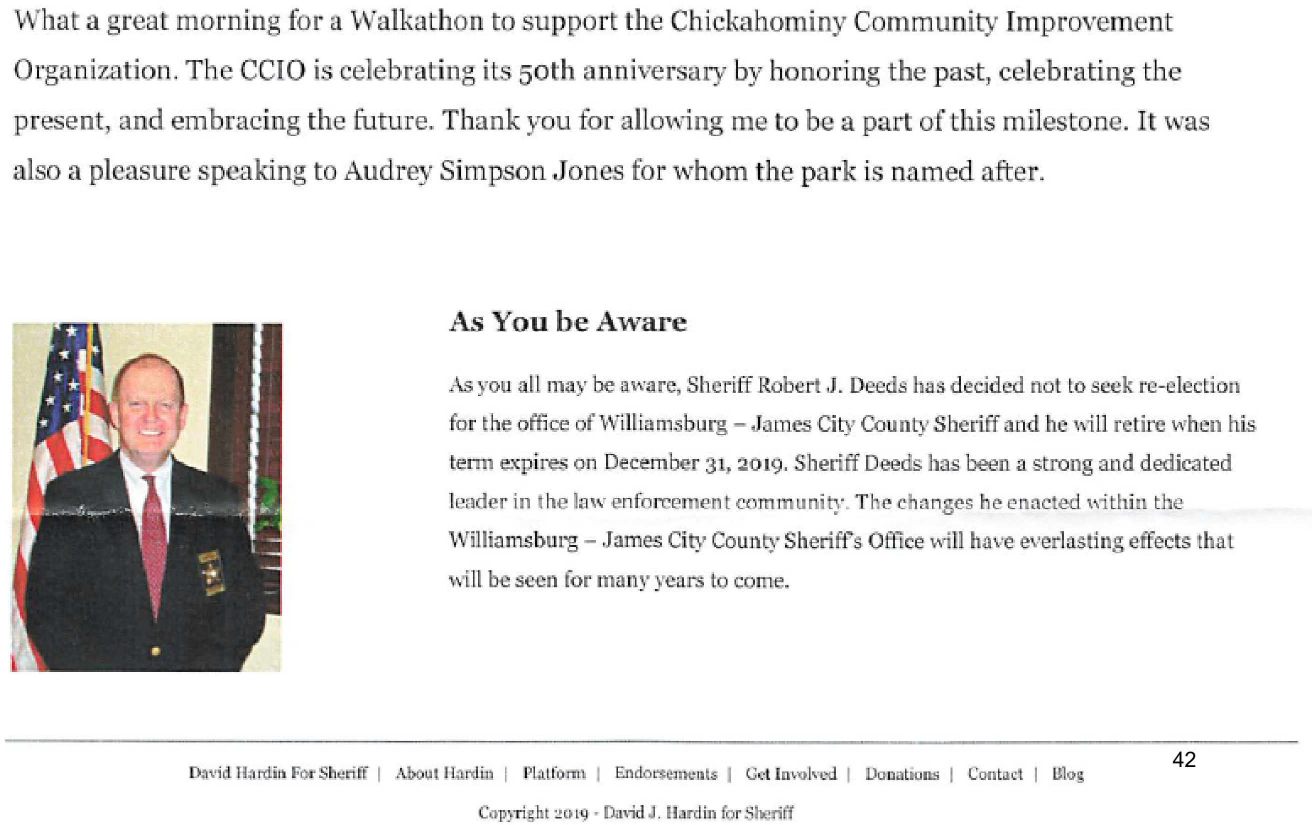


Tell us WHERE and WHEN you saw the ad(s). *Add additional pages if needed.*

NO AUTHORIZED By on His website

David Hardin for sheriff.com

Webpage as of Oct. 25, 2019



What a great morning for a Walkathon to support the Chickahominy Community Improvement Organization. The CCIO is celebrating its 50th anniversary by honoring the past, celebrating the present, and embracing the future. Thank you for allowing me to be a part of this milestone. It was also a pleasure speaking to Audrey Simpson Jones for whom the park is named after.

As You be Aware

As you all may be aware, Sheriff Robert J. Deeds has decided not to seek re-election for the office of Williamsburg – James City County Sheriff and he will retire when his term expires on December 31, 2019. Sheriff Deeds has been a strong and dedicated leader in the law enforcement community. The changes he enacted within the Williamsburg – James City County Sheriff's Office will have everlasting effects that will be seen for many years to come.

David Hardin For Sheriff | About Hardin | Platform | Endorsements | Get Involved | Donations | Contact | Blog

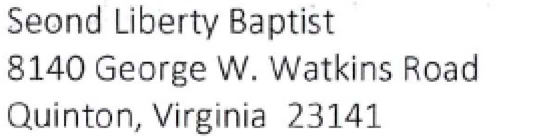
Copyright 2019 - David J. Hardin for Sheriff

8. Friends of Joe Dombroski CC-19-01133

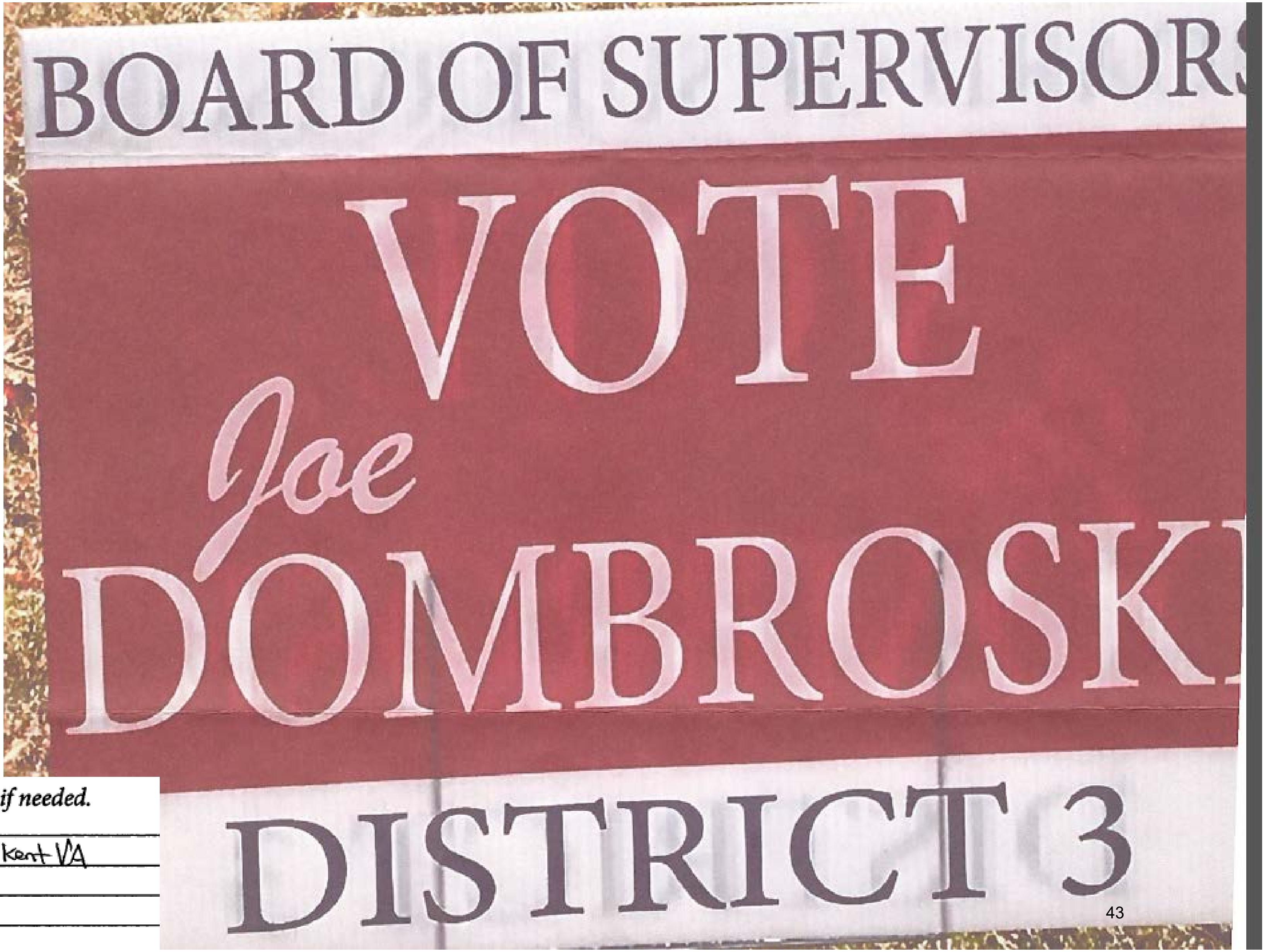
One sign

Violation Date Sept. 20, 2019

Return address on envelope



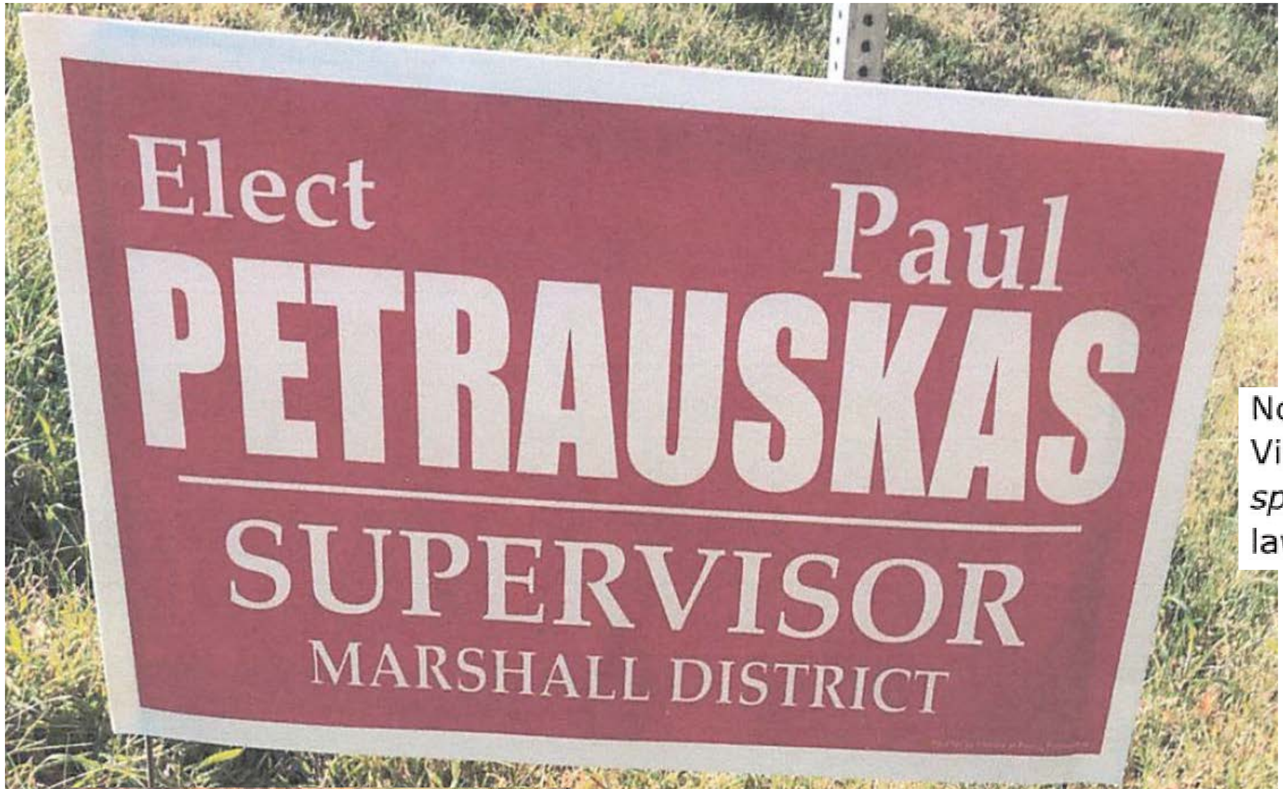
Seond Liberty Baptist
8140 George W. Watkins Road
Quinton, Virginia 23141



Tell us WHERE and WHEN you saw the ad(s). ***Add additional pages if needed.***

9-20-19 to present. New Kent Highway, New Kent VA
Also Vineyard Parkway (Rt 106)
numerous Signs no "Paid by"

9. Friends of Paul Petrauskas CC-19-00793

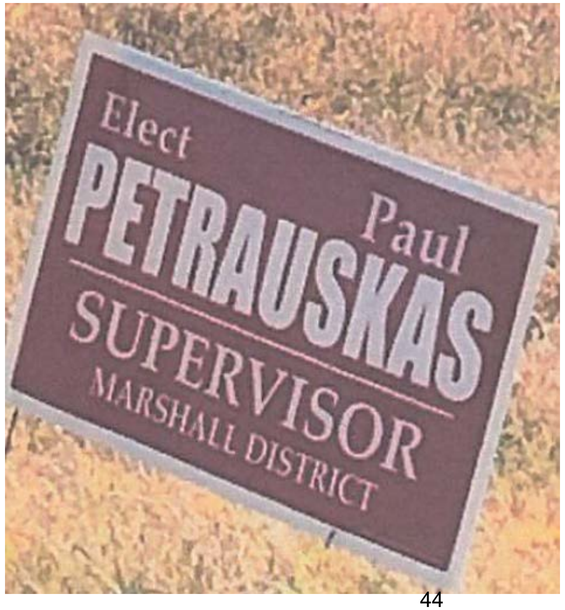


10 signs

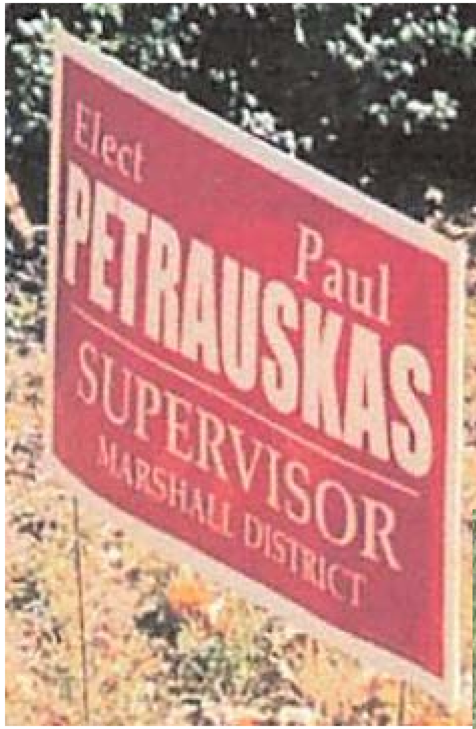
Complaint by Nelson Warfield via snail mail

Violation Date October 15, 2019

None of these signs display the information required by law in the Code of Virginia: § *24.2-956. Requirements for print media advertisements sponsored by a candidate campaign committee* or as elsewhere specified in laws of the Commonwealth.



Elect
Paul
PETRAUSKAS
SUPERVISOR
MARSHALL DISTRICT


Elect
Paul
PETRAUSKAS
SUPERVISOR
MARSHALL DISTRICT

Elect
Paul
PETRAUSKAS
SUPERVISOR
MARSHALL DISTRICT

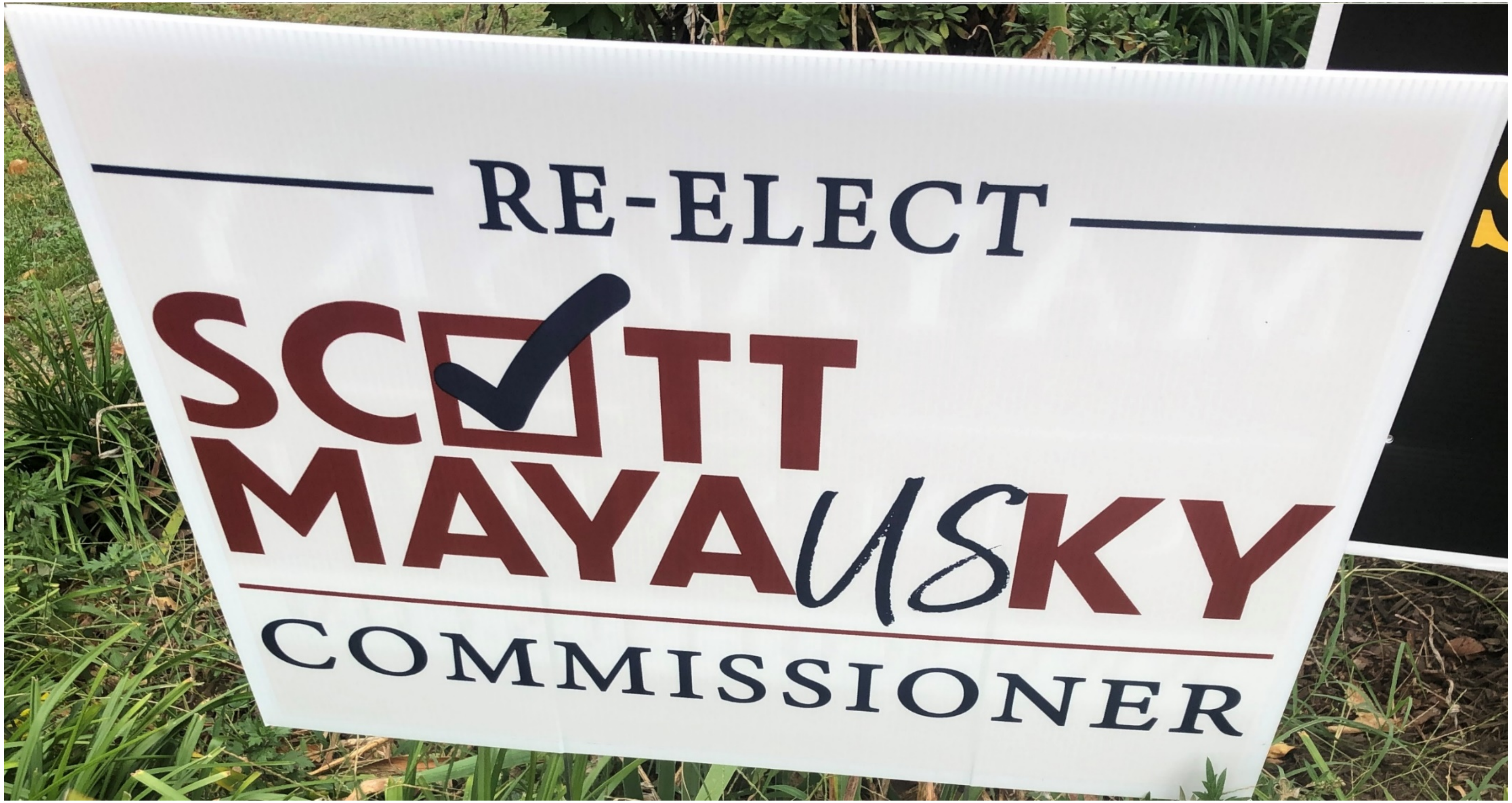
PETRAUSKAS
SUPERVISOR

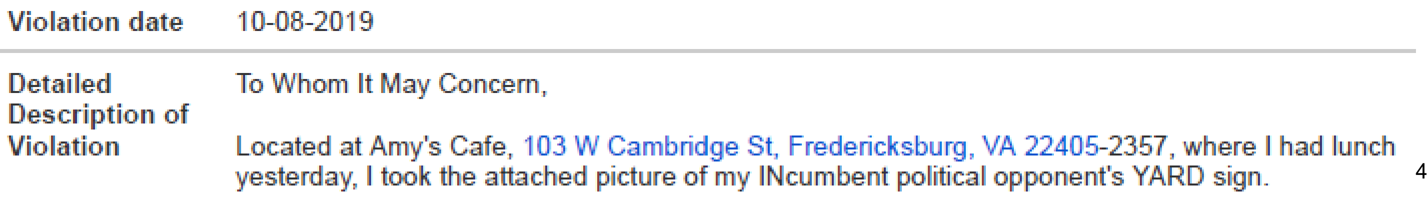
Elect
Paul
PETRAUSKAS
SUPERVISOR
MARSHALL DISTRICT

10. Friends of Scott Mayausky CC-13-00569

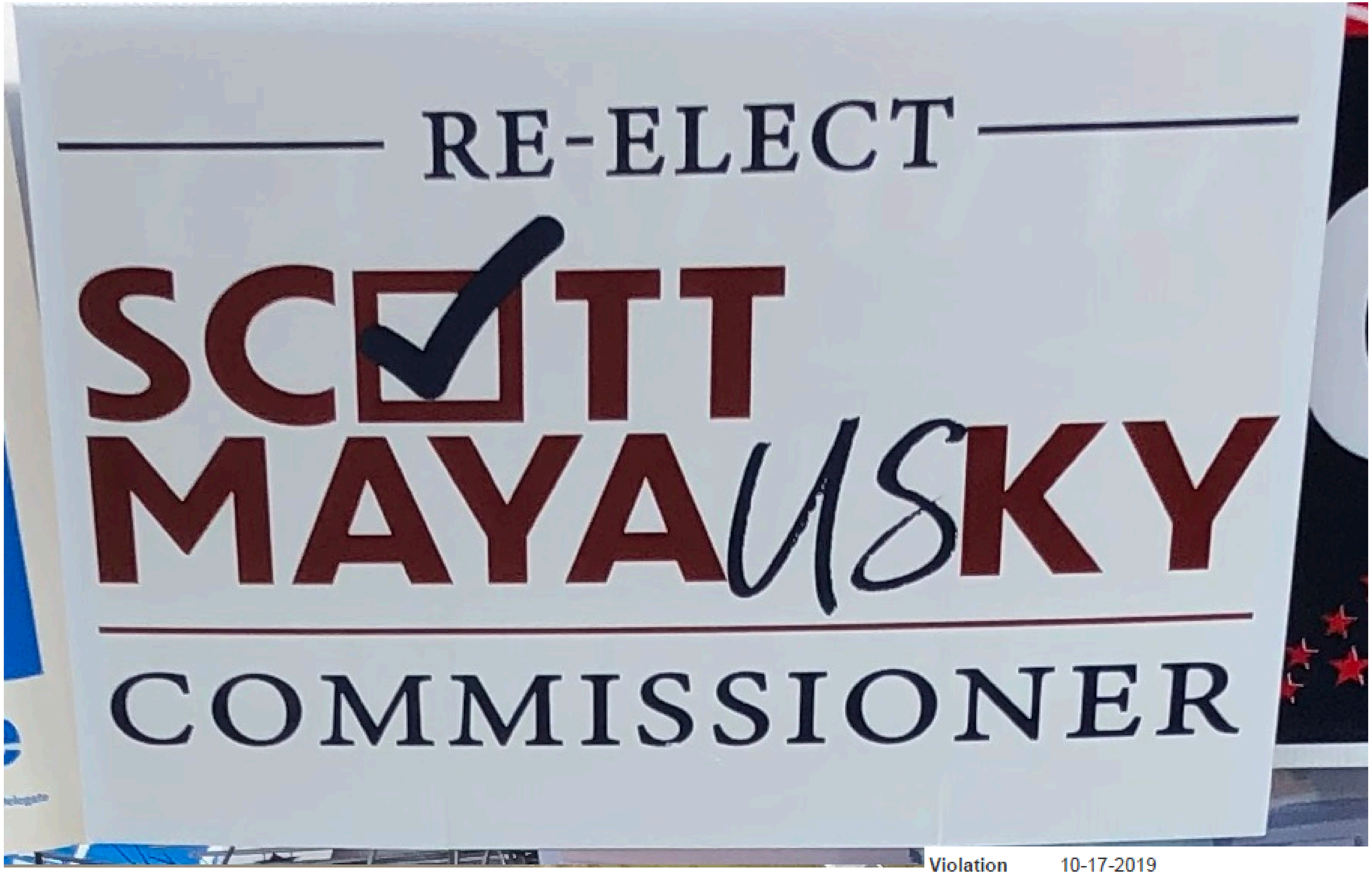
3 Signs Complaints

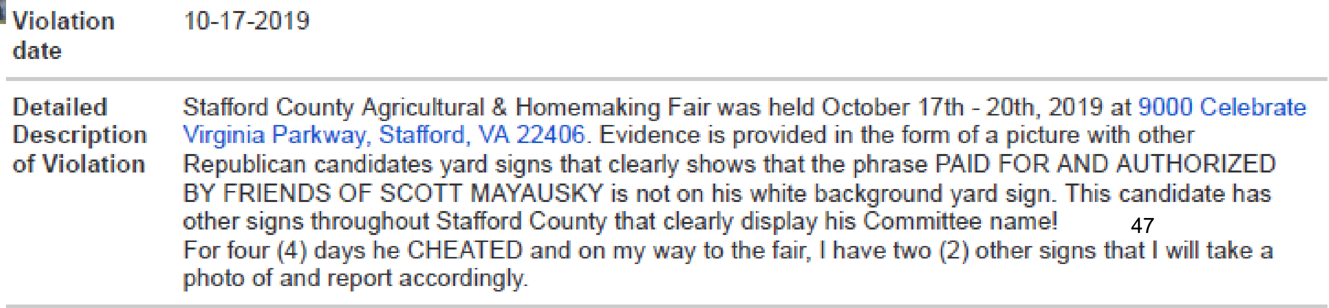
SBYA Online Complaints all by Paul Waldowski



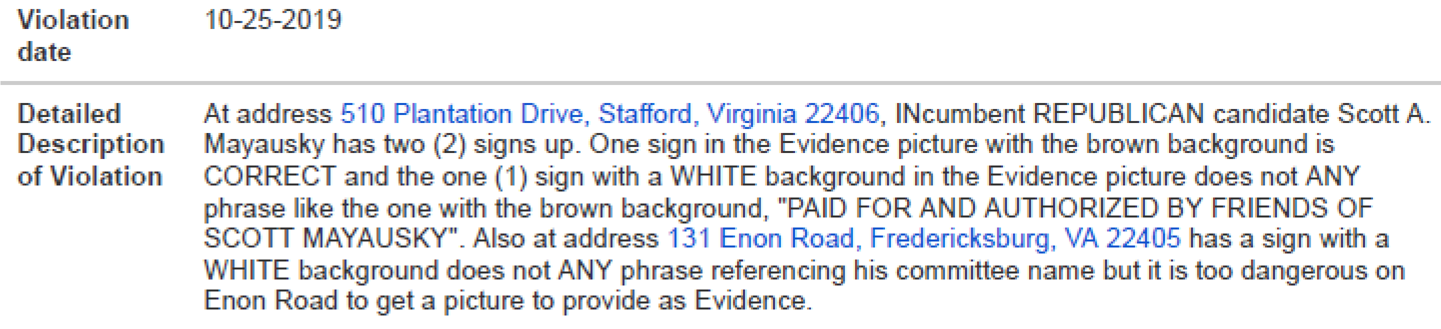


Violation date	10-08-2019
Detailed Description of Violation	To Whom It May Concern, Located at Amy's Cafe, 103 W Cambridge St, Fredericksburg, VA 22405-2357, where I had lunch yesterday, I took the attached picture of my INcumbent political opponent's YARD sign.

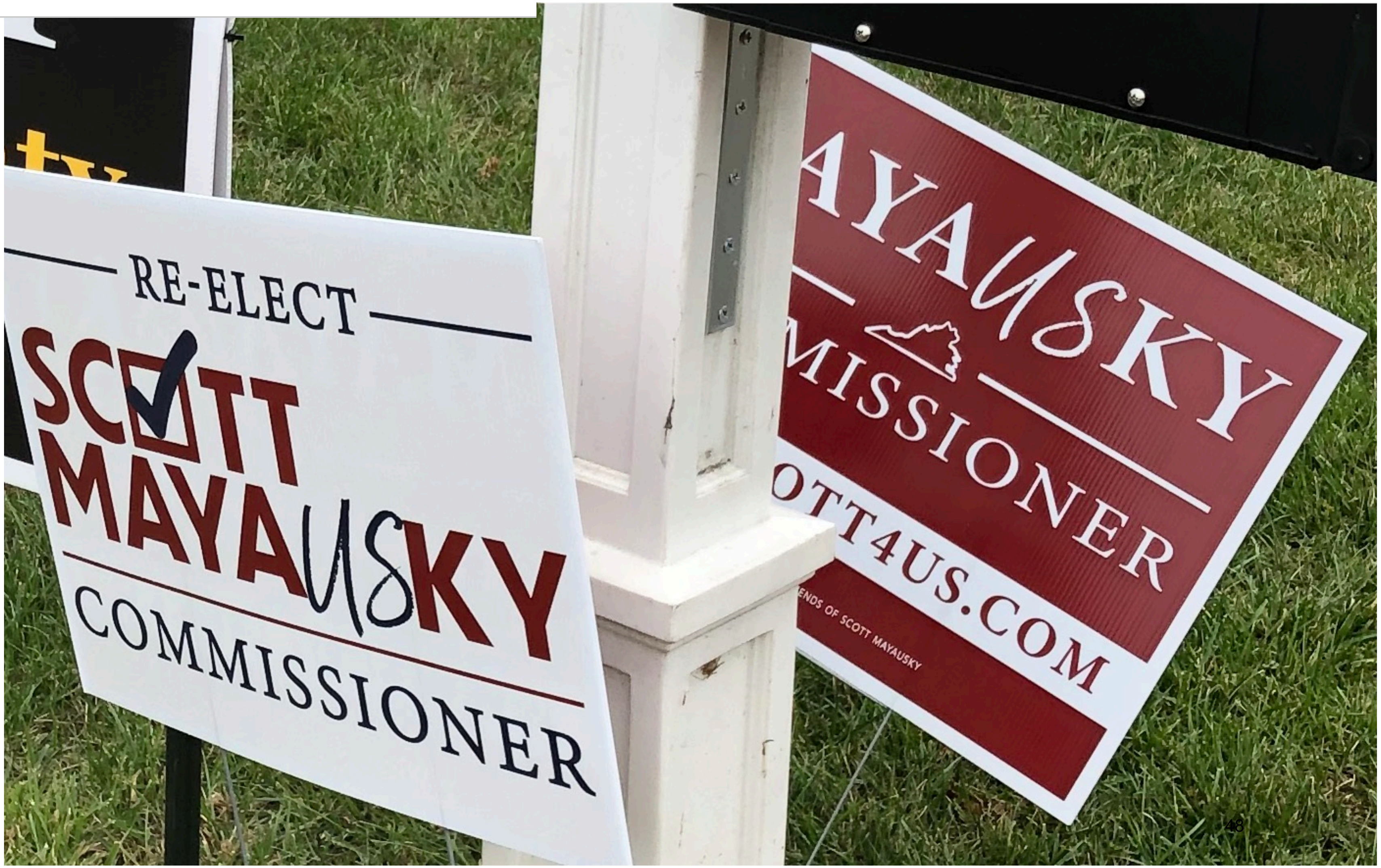




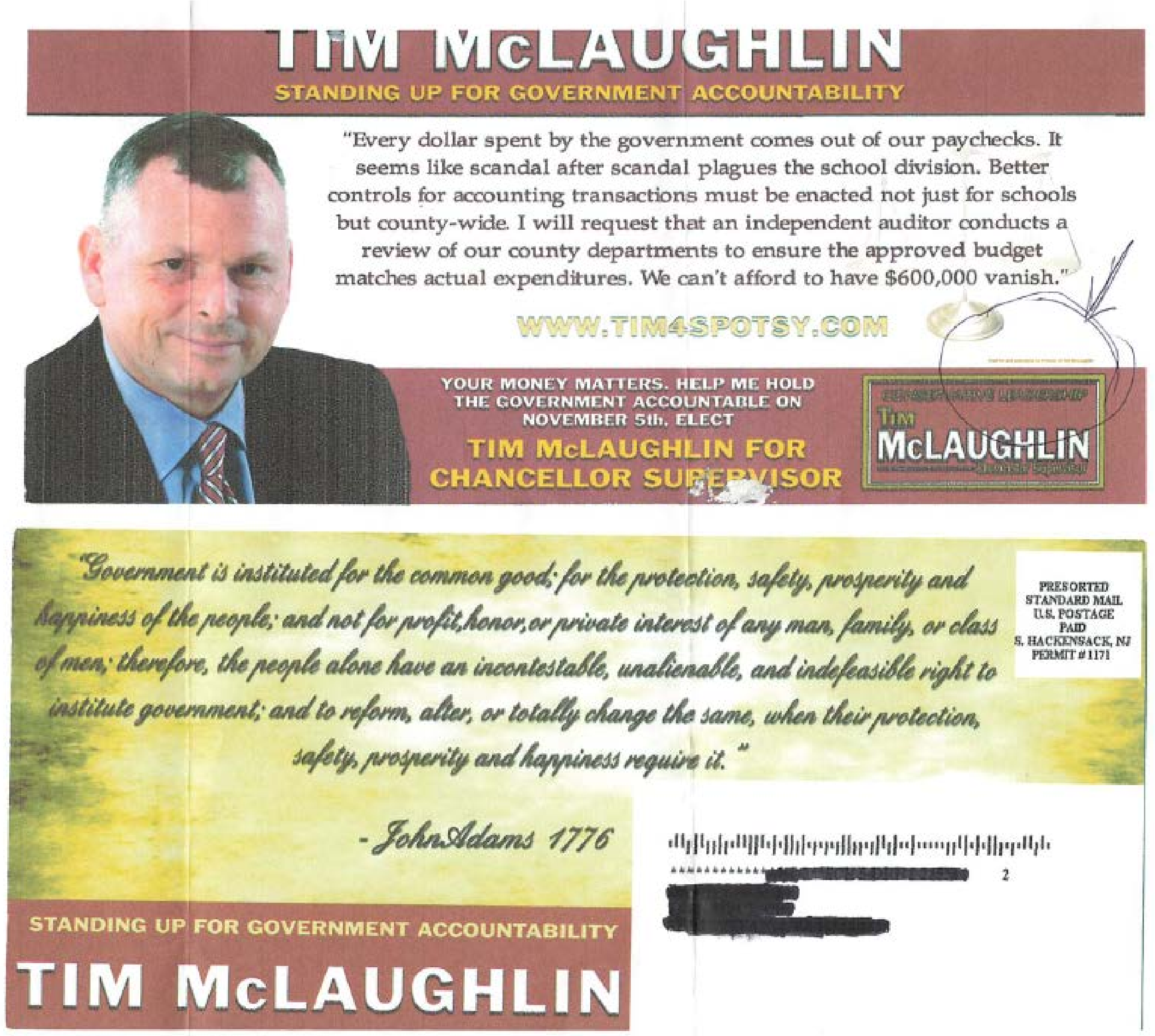
Violation date	10-17-2019
Detailed Description of Violation	Stafford County Agricultural & Homemaking Fair was held October 17th - 20th, 2019 at 9000 Celebrate Virginia Parkway, Stafford, VA 22406. Evidence is provided in the form of a picture with other Republican candidates yard signs that clearly shows that the phrase PAID FOR AND AUTHORIZED BY FRIENDS OF SCOTT MAYAUSKY is not on his white background yard sign. This candidate has other signs throughout Stafford County that clearly display his Committee name! For four (4) days he CHEATED and on my way to the fair, I have two (2) other signs that I will take a photo of and report accordingly.



Violation date	10-25-2019
Detailed Description of Violation	At address 510 Plantation Drive, Stafford, Virginia 22406, INcumbent REPUBLICAN candidate Scott A. Mayausky has two (2) signs up. One sign in the Evidence picture with the brown background is CORRECT and the one (1) sign with a WHITE background in the Evidence picture does not ANY phrase like the one with the brown background, "PAID FOR AND AUTHORIZED BY FRIENDS OF SCOTT MAYAUSKY". Also at address 131 Enon Road, Fredericksburg, VA 22405 has a sign with a WHITE background does not ANY phrase referencing his committee name but it is too dangerous on Enon Road to get a picture to provide as Evidence.



11. Friends of Tim McLaughlin CC-15-00154



TIM McLAUGHLIN

STANDING UP FOR GOVERNMENT ACCOUNTABILITY

"Every dollar spent by the government comes out of our paychecks. It seems like scandal after scandal plagues the school division. Better controls for accounting transactions must be enacted not just for schools but county-wide. I will request that an independent auditor conducts a review of our county departments to ensure the approved budget matches actual expenditures. We can't afford to have $600,000 vanish."

WWW.TIM4SPOTSY.COM

YOUR MONEY MATTERS. HELP ME HOLD THE GOVERNMENT ACCOUNTABLE ON NOVEMBER 5th. ELECT

TIM McLAUGHLIN FOR CHANCELLOR SUPERVISOR

"Government is instituted for the common good; for the protection, safety, prosperity and happiness of the people; and not for profit,honor,or private interest of any man, family, or class of men; therefore, the people alone have an incontestable, unalienable, and indefeasible right to institute government; and to reform, alter, or totally change the same, when their protection, safety, prosperity and happiness require it."

- JohnAdams 1776

PRESORTED
STANDARD MAIL
U.S. POSTAGE
PAID
S. HACKENSACK, NJ
PERMIT # 1171

[redacted]

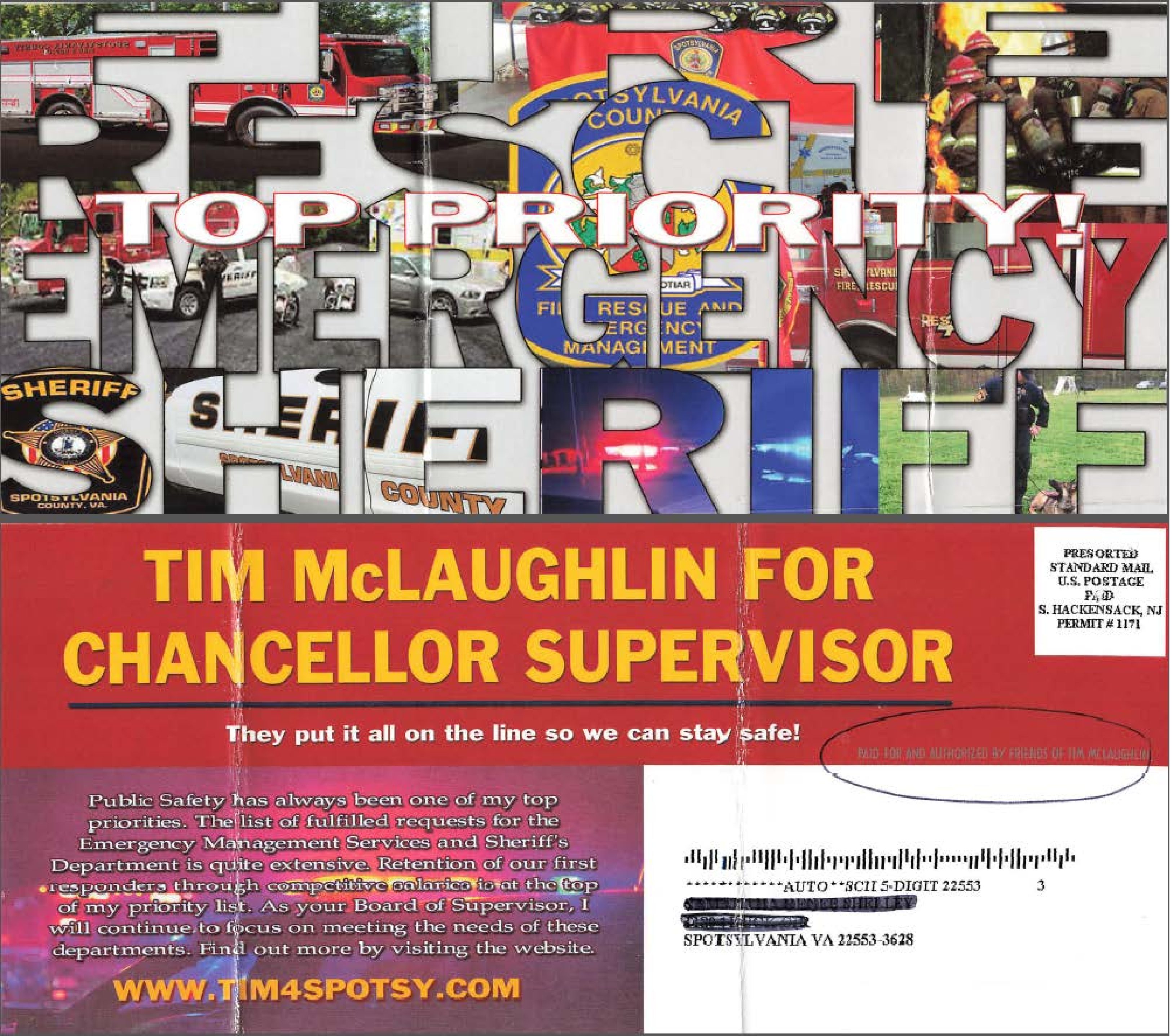
STANDING UP FOR GOVERNMENT ACCOUNTABILITY

TIM McLAUGHLIN

2 complaints

3. Tell us WHERE and WHEN you saw the ad(s). *Add additional pages if needed.*

This came to my mailbox. I had to search where it said "Friends of Tim McLaughlin". Then I still couldn't see it without a magnifying glass.


FIRE
RESCUE
EMERGENCY
SHERIFF
TOP PRIORITY!

TIM McLAUGHLIN FOR CHANCELLOR SUPERVISOR

They put it all on the line so we can stay safe!

PAID FOR AND AUTHORIZED BY FRIENDS OF TIM MCLAUGHLIN

PRESORTED
STANDARD MAIL
U.S. POSTAGE
PAID
S. HACKENSACK, NJ
PERMIT # 1171

Public Safety has always been one of my top priorities. The list of fulfilled requests for the Emergency Management Services and Sheriff's Department is quite extensive. Retention of our first responders through competitive salaries is at the top of my priority list. As your Board of Supervisor, I will continue to focus on meeting the needs of these departments. Find out more by visiting the website.

WWW.TIM4SPOTSY.COM

************AUTO**SCH 5-DIGIT 22553 3
[redacted]
SPOTSYLVANIA VA 22553-3628

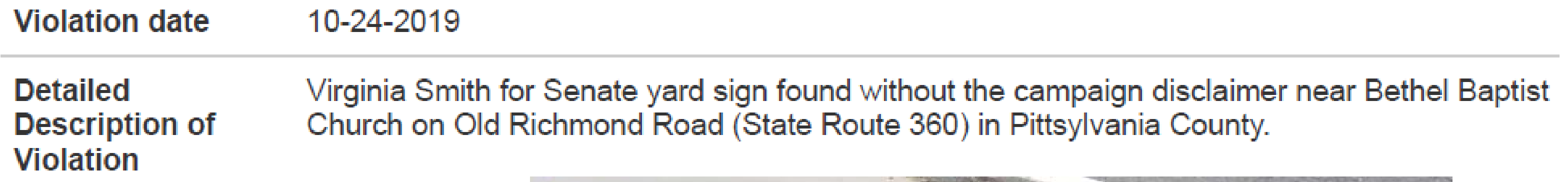
Came in mail on 9/28/19

barely see disclosure.

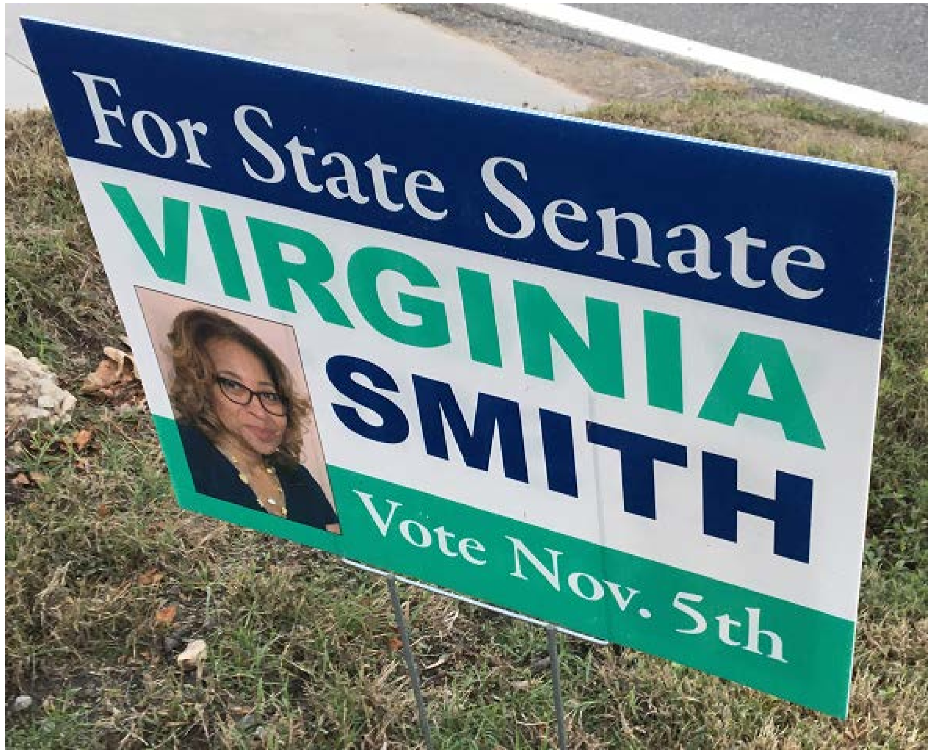
12. Friends of Virginia CC-19-00343

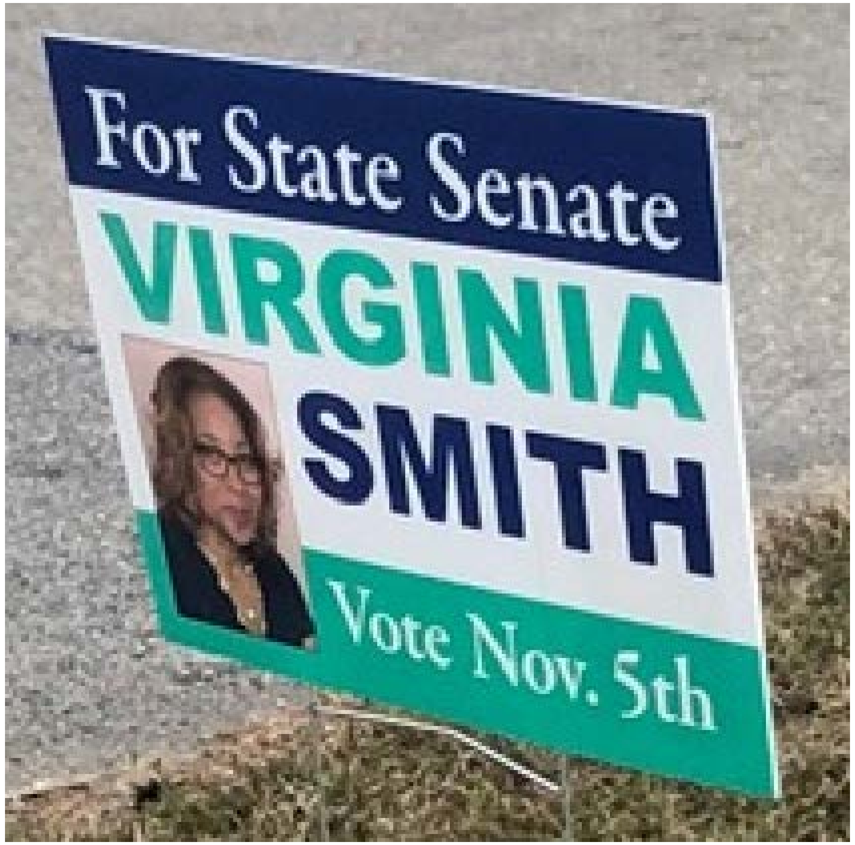
4 signs

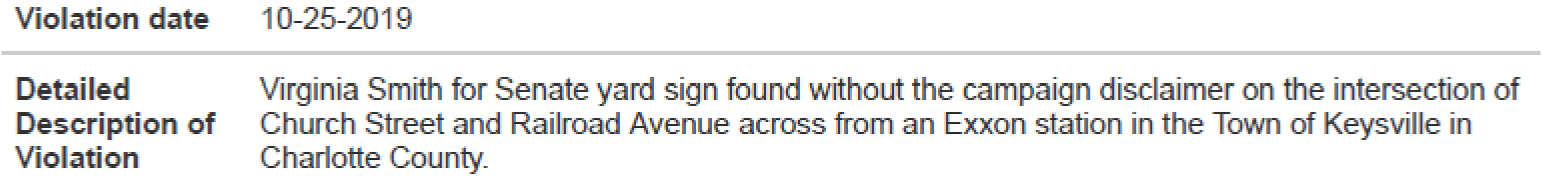
Complaint by William Pace



Violation date	10-24-2019
Detailed Description of Violation	Virginia Smith for Senate yard sign found without the campaign disclaimer near Bethel Baptist Church on Old Richmond Road (State Route 360) in Pittsylvania County.

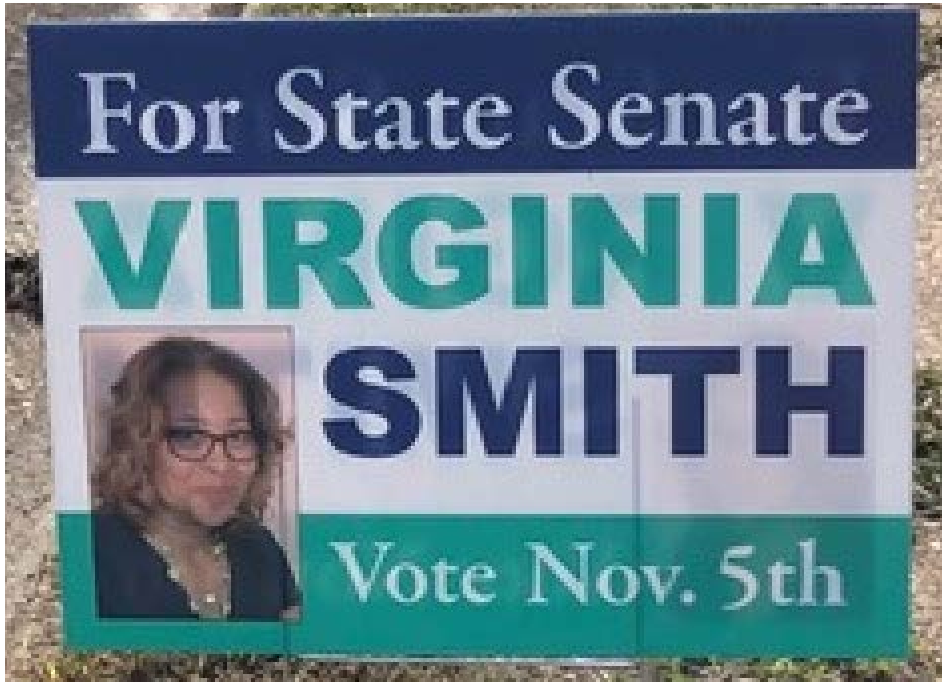


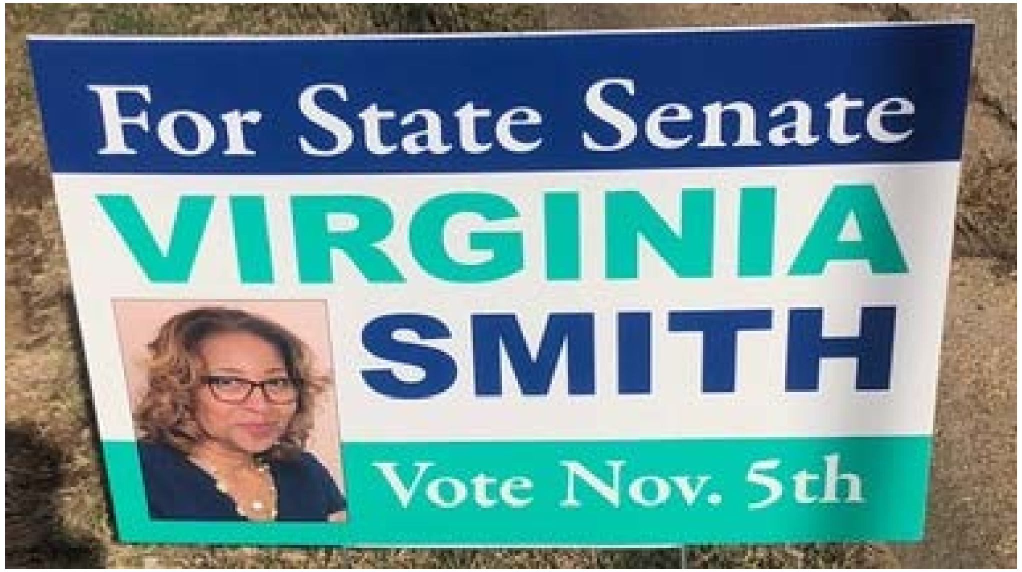




Violation date	10-25-2019
Detailed Description of Violation	Virginia Smith for Senate yard sign found without the campaign disclaimer on the intersection of Church Street and Railroad Avenue across from an Exxon station in the Town of Keysville in Charlotte County.

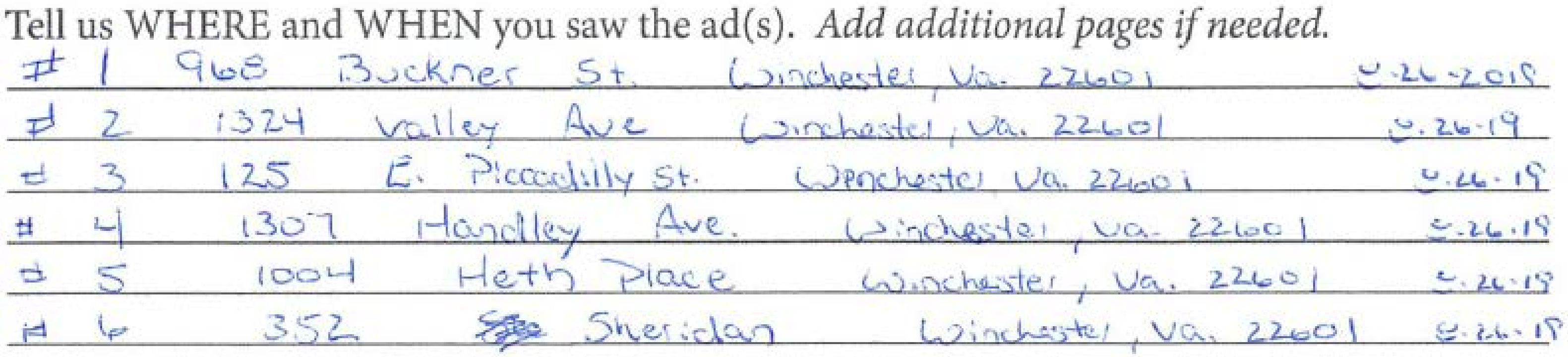
Violation date	10-26-2019
Detailed Description of Violation	Virginia Smith for Senate yard sign (first of two) found without the campaign disclaimer in front of a Food Lion on Old Kings Highway in the Town of Keysville in Charlotte County.





Violation date	10-26-2019
Detailed Description of Violation	Virginia Smith for Senate yard sign (second of two) found without the campaign disclaimer in front of a Food Lion on Old Kings Highway in the Town of Keysville in Charlotte County.

13. Friends of Will Gardner CC-19-00541



Tell us WHERE and WHEN you saw the ad(s). *Add additional pages if needed.*

1 968 Buckner St. Winchester, Va. 22601 8-26-2019

2 1324 Valley Ave Winchester, Va. 22601 8.26-19

3 125 E. Piccadilly St. Winchester Va. 22601 8.26.19

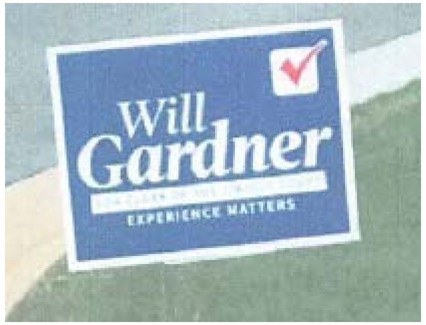
4 1307 Handley Ave. Winchester, Va. 22601 8.26.19

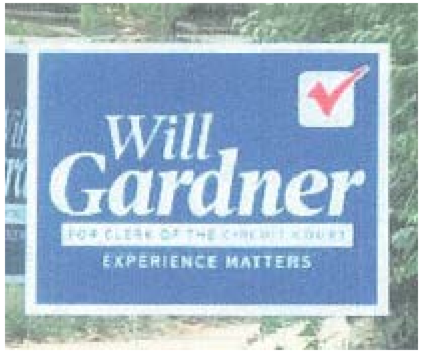
5 1004 Heth Place Winchester, Va. 22601 8.26.19

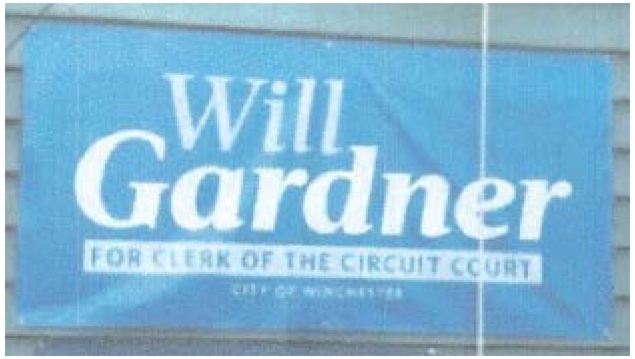
6 352 Sheridan Winchester, Va. 22601 8.26.19

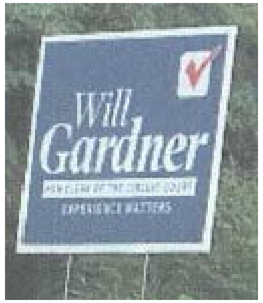
5 Yard Sign, 1 banner

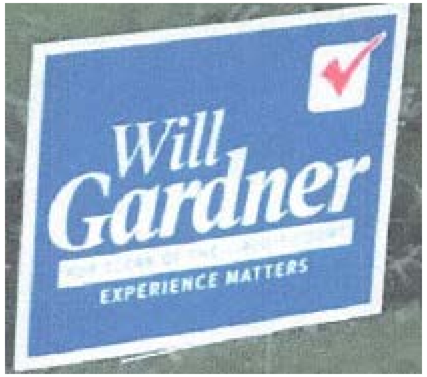
Anonymous





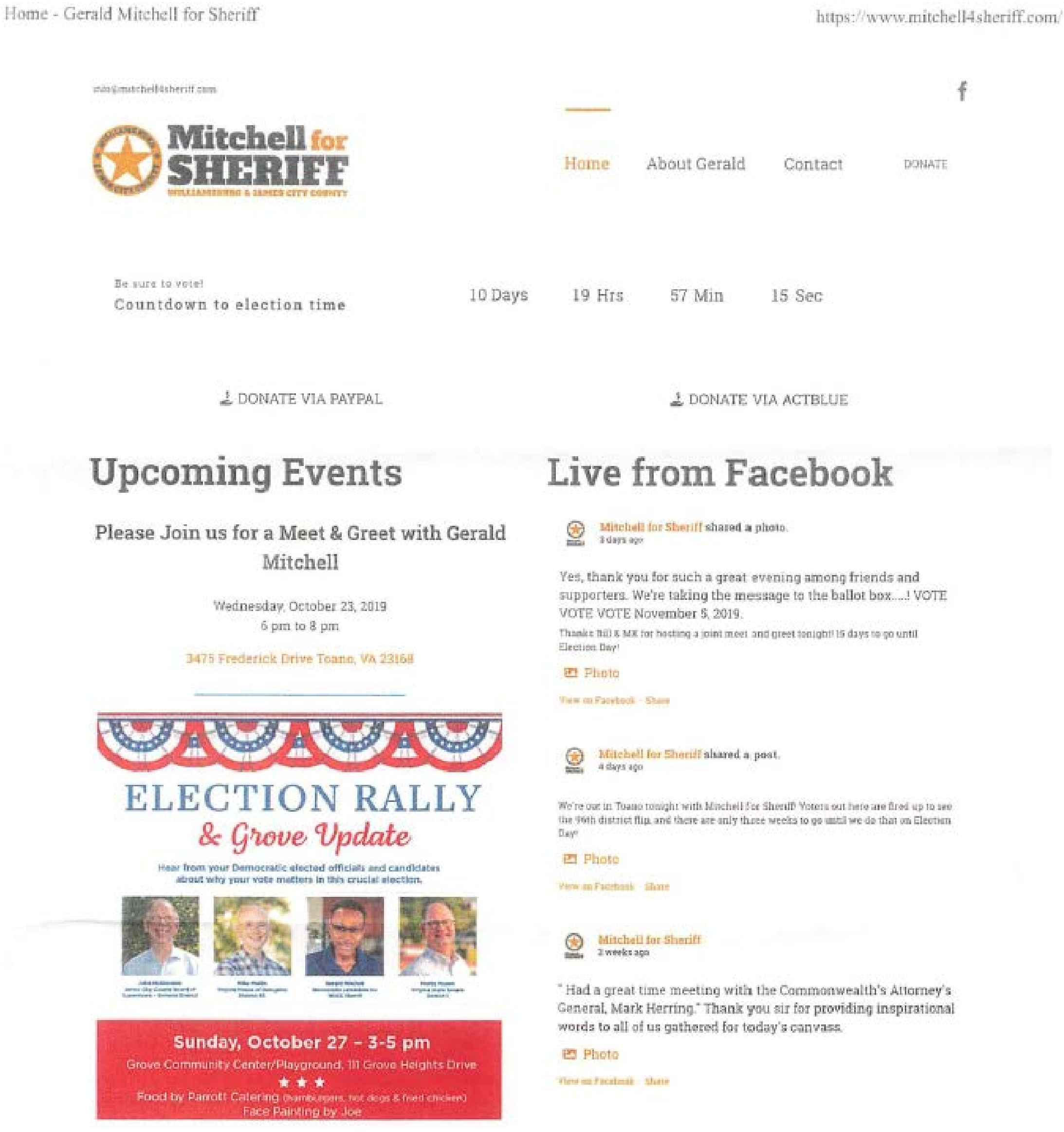






14. Gerald Mitchell for Sheriff CC-19-00884

1 webpage



Home - Gerald Mitchell for Sheriff

https://www.mitchell4sheriff.com/

Mitchell for SHERIFF
WILLIAMSBURG & JAMES CITY COUNTY
Home
About Gerald
Contact
DONATE

Be sure to vote!
Countdown to election time

10 Days 19 Hrs 57 Min 15 Sec

DONATE VIA PAYPAL

DONATE VIA ACTBLUE

Upcoming Events

Please Join us for a Meet & Greet with Gerald Mitchell

Wednesday, October 23, 2019
6 pm to 8 pm

3475 Frederick Drive Toano, VA 23168

ELECTION RALLY
& Grove Update
Hear from your Democratic elected officials and candidates about why your vote matters in this crucial election.
Sunday, October 27 – 3-5 pm
Grove Community Center/Playground, 111 Grove Heights Drive
★ ★ ★
Food by Parrott Catering (hamburgers, hot dogs & fried chicken)
Face Painting by Joe

Live from Facebook

Mitchell for Sheriff shared a photo.
3 days ago

Yes, thank you for such a great evening among friends and supporters. We're taking the message to the ballot box....! VOTE VOTE VOTE November 5, 2019.

Thanks Bill & MK for hosting a joint meet and greet tonight! 15 days to go until Election Day!

Photo

View on Facebook · Share

Mitchell for Sheriff shared a post.
4 days ago

We're out in Toano tonight with Mitchell for Sheriff! Voters out here are fired up to see the 96th district flip, and there are only three weeks to go until we do that on Election Day!

Photo

View on Facebook · Share

Mitchell for Sheriff
3 weeks ago

" Had a great time meeting with the Commonwealth's Attorney's General, Mark Herring." Thank you sir for providing inspirational words to all of us gathered for today's canvass.

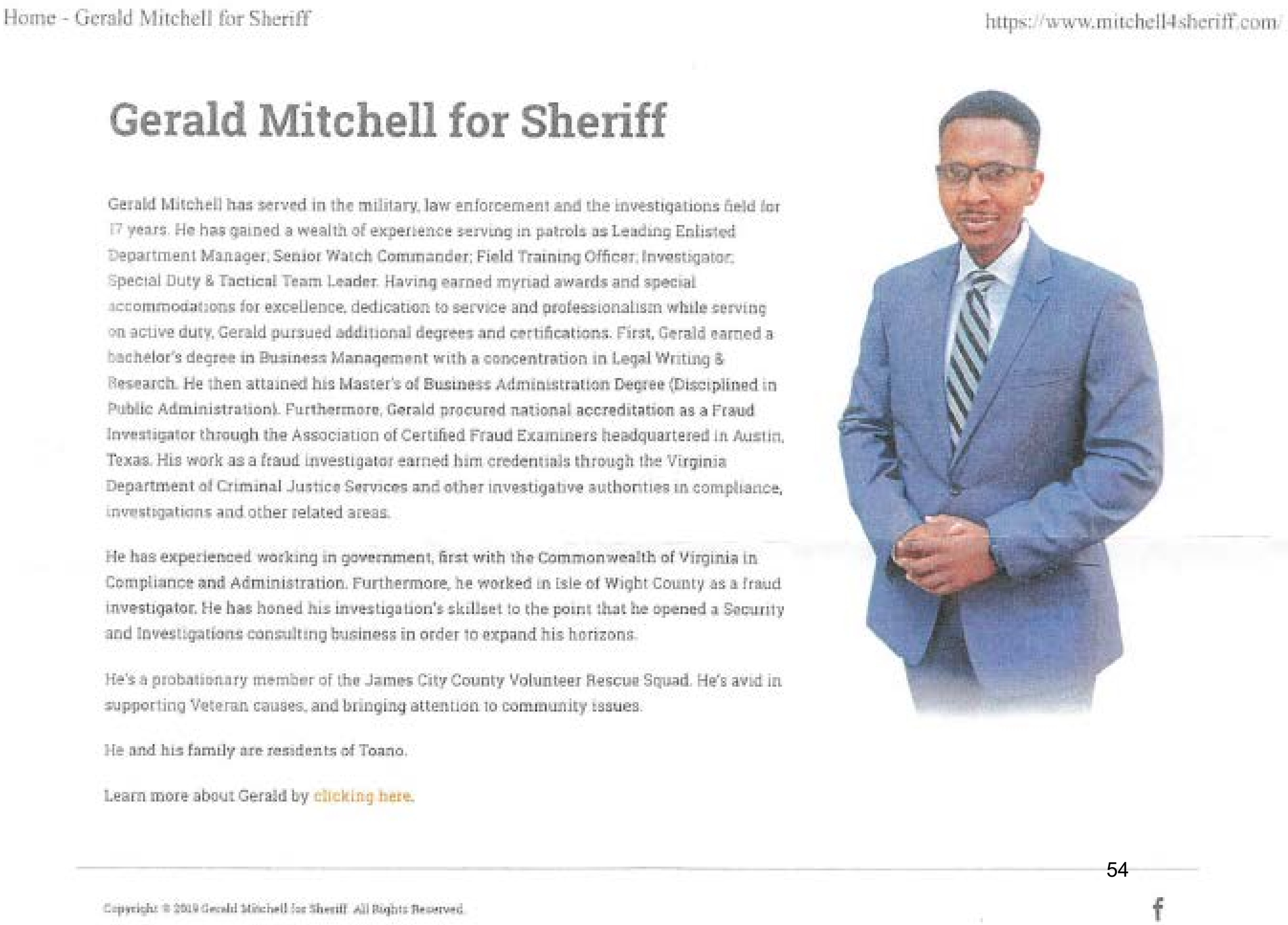
Photo

View on Facebook · Share

10/25/2019, 11:02 AM

Tell us WHERE and WHEN you saw the ad(s). *Add additional pages if needed.*

No authorized + Paid
for by on website



Home - Gerald Mitchell for Sheriff

https://www.mitchell4sheriff.com/

Gerald Mitchell for Sheriff

Gerald Mitchell has served in the military, law enforcement and the investigations field for 17 years. He has gained a wealth of experience serving in patrols as Leading Enlisted Department Manager, Senior Watch Commander; Field Training Officer; Investigator; Special Duty & Tactical Team Leader. Having earned myriad awards and special accommodations for excellence, dedication to service and professionalism while serving on active duty, Gerald pursued additional degrees and certifications. First, Gerald earned a bachelor's degree in Business Management with a concentration in Legal Writing & Research. He then attained his Master's of Business Administration Degree (Disciplined in Public Administration). Furthermore, Gerald procured national accreditation as a Fraud Investigator through the Association of Certified Fraud Examiners headquartered in Austin, Texas. His work as a fraud investigator earned him credentials through the Virginia Department of Criminal Justice Services and other investigative authorities in compliance, investigations and other related areas.

He has experienced working in government, first with the Commonwealth of Virginia in Compliance and Administration. Furthermore, he worked in Isle of Wight County as a fraud investigator. He has honed his investigation's skillset to the point that he opened a Security and Investigations consulting business in order to expand his horizons.

He's a probationary member of the James City County Volunteer Rescue Squad. He's avid in supporting Veteran causes, and bringing attention to community issues.

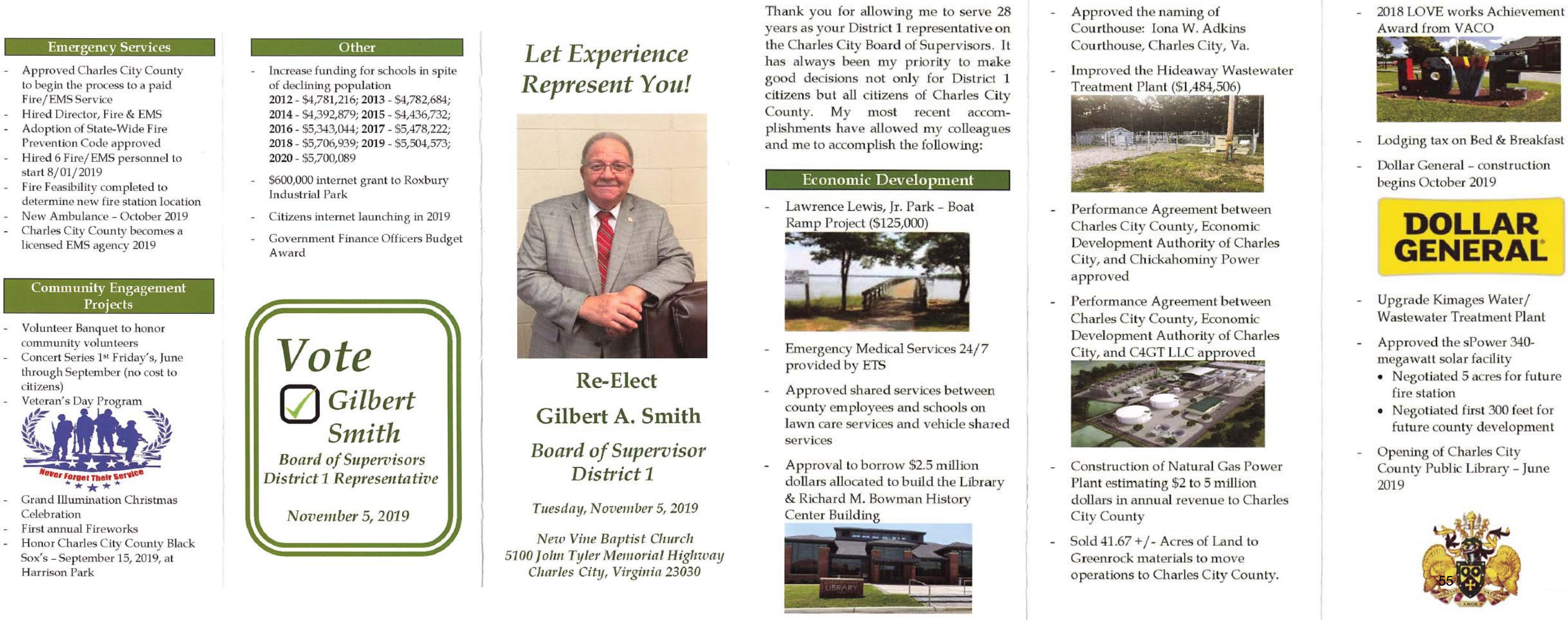
He and his family are residents of Toano.

Learn more about Gerald by clicking here.

15. Gilbert A. Smith

1 pamphlet

Delivered in person by Helen Payne-Jones October 17, 2019



Emergency Services

- Approved Charles City County to begin the process to a paid Fire/EMS Service
- Hired Director, Fire & EMS
- Adoption of State-Wide Fire Prevention Code approved
- Hired 6 Fire/EMS personnel to start 8/01/2019
- Fire Feasibility completed to determine new fire station location
- New Ambulance – October 2019
- Charles City County becomes a licensed EMS agency 2019

Community Engagement Projects

- Volunteer Banquet to honor community volunteers
- Concert Series 1st Friday's, June through September (no cost to citizens)
- Veteran's Day Program
- Grand Illumination Christmas Celebration
- First annual Fireworks
- Honor Charles City County Black Sox's – September 15, 2019, at Harrison Park

Other

- Increase funding for schools in spite of declining population **2012** - $4,781,216; **2013** - $4,782,684; **2014** - $4,392,879; **2015** - $4,436,732; **2016** - $5,343,044; **2017** - $5,478,222; **2018** - $5,706,939; **2019** - $5,504,573; **2020** - $5,700,089
- $600,000 internet grant to Roxbury Industrial Park
- Citizens internet launching in 2019
- Government Finance Officers Budget Award

Vote

☑ *Gilbert Smith*

Board of Supervisors District 1 Representative

November 5, 2019

Let Experience Represent You!

Re-Elect

Gilbert A. Smith

Board of Supervisor District 1

Tuesday, November 5, 2019

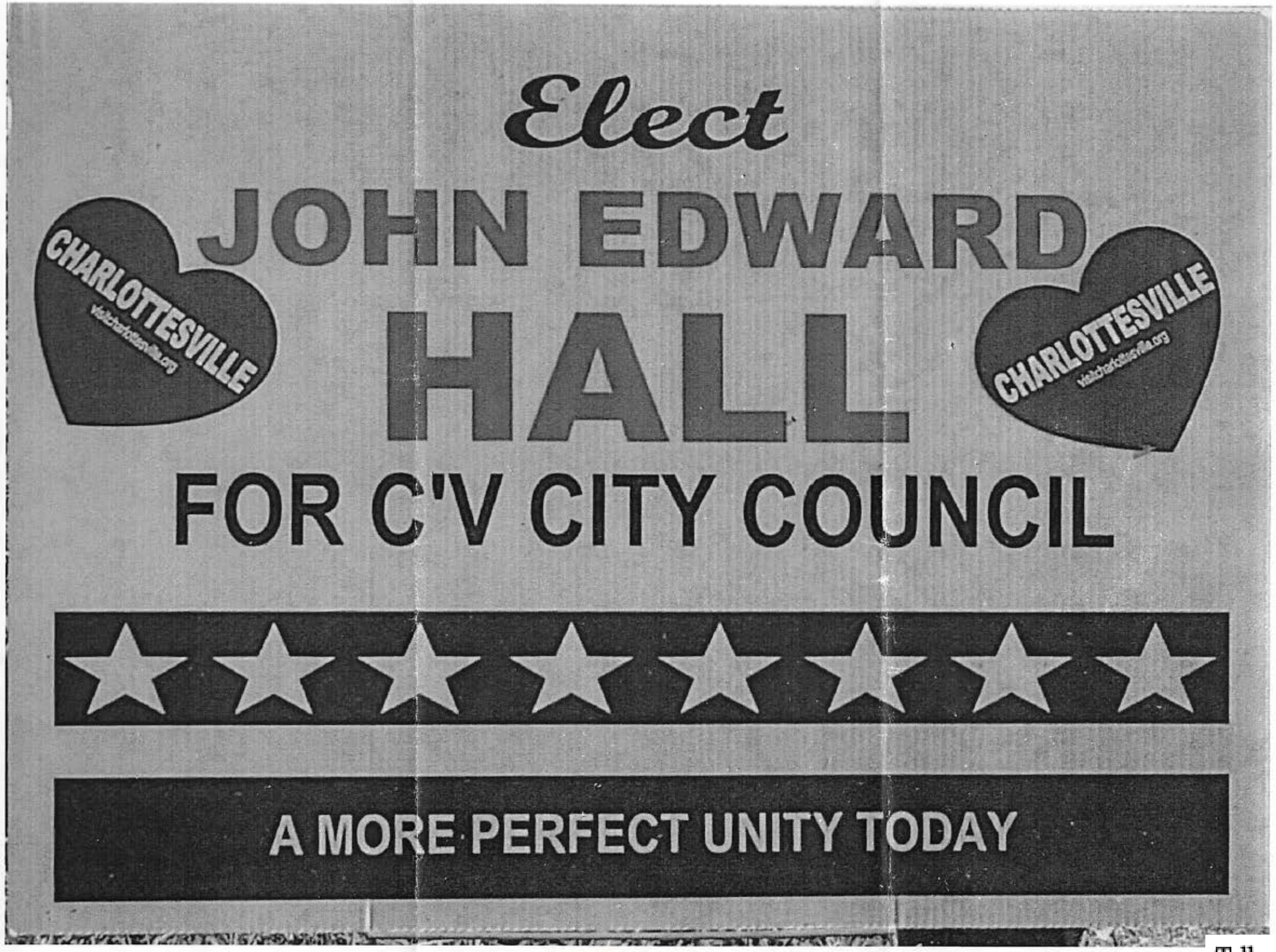
New Vine Baptist Church
5100 John Tyler Memorial Highway
Charles City, Virginia 23030

Thank you for allowing me to serve 28 years as your District 1 representative on the Charles City Board of Supervisors. It has always been my priority to make good decisions not only for District 1 citizens but all citizens of Charles City County. My most recent accomplishments have allowed my colleagues and me to accomplish the following:

Economic Development

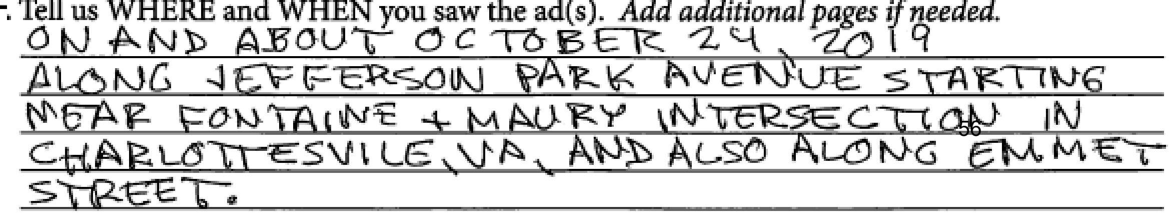
- Lawrence Lewis, Jr. Park – Boat Ramp Project ($125,000)
- Emergency Medical Services 24/7 provided by ETS
- Approved shared services between county employees and schools on lawn care services and vehicle shared services
- Approval to borrow $2.5 million dollars allocated to build the Library & Richard M. Bowman History Center Building
- Approved the naming of Courthouse: Iona W. Adkins Courthouse, Charles City, Va.
- Improved the Hideaway Wastewater Treatment Plant ($1,484,506)
- Performance Agreement between Charles City County, Economic Development Authority of Charles City, and Chickahominy Power approved
- Performance Agreement between Charles City County, Economic Development Authority of Charles City, and C4GT LLC approved
- Construction of Natural Gas Power Plant estimating $2 to 5 million dollars in annual revenue to Charles City County
- Sold 41.67 +/- Acres of Land to Greenrock materials to move operations to Charles City County.
- 2018 LOVE works Achievement Award from VACO
- Lodging tax on Bed & Breakfast
- Dollar General – construction begins October 2019
- Upgrade Kimages Water/ Wastewater Treatment Plant
- Approved the sPower 340-megawatt solar facility
  - Negotiated 5 acres for future fire station
  - Negotiated first 300 feet for future county development
- Opening of Charles City County Public Library – June 2019

16. John Edward Hall



One sign, one side

Anonymous



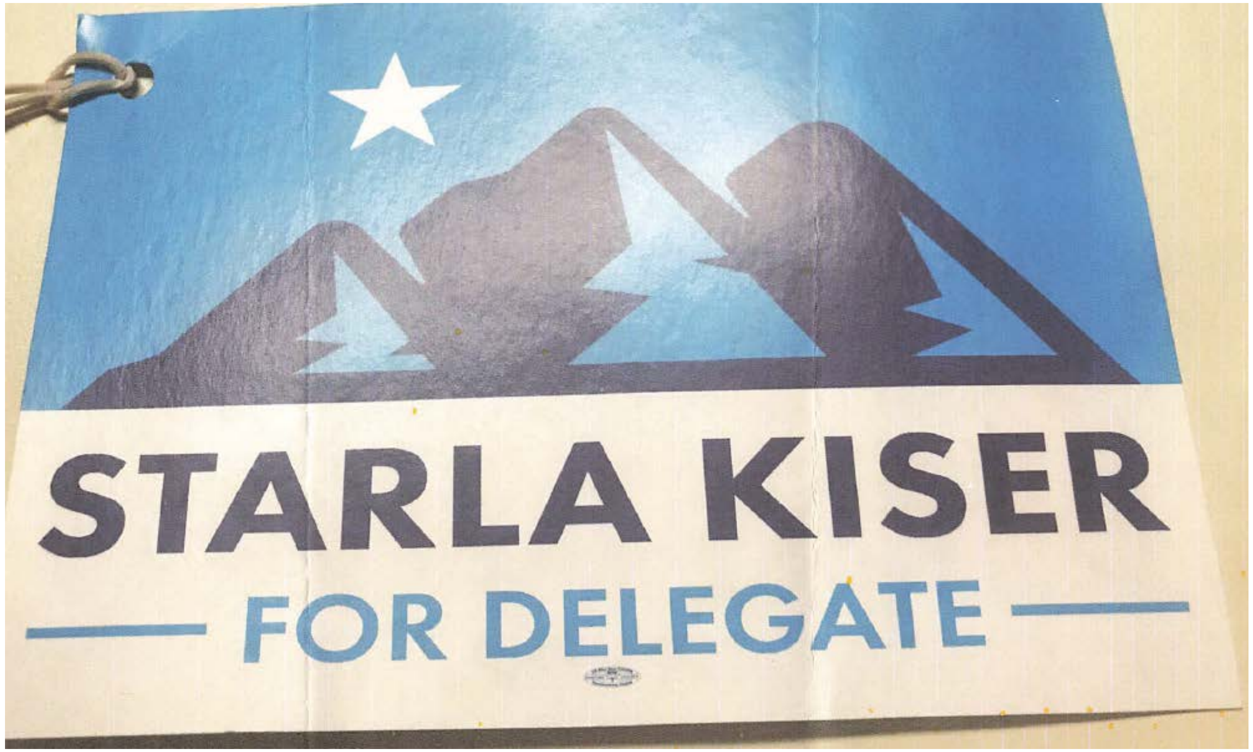
. Tell us WHERE and WHEN you saw the ad(s). *Add additional pages if needed.*

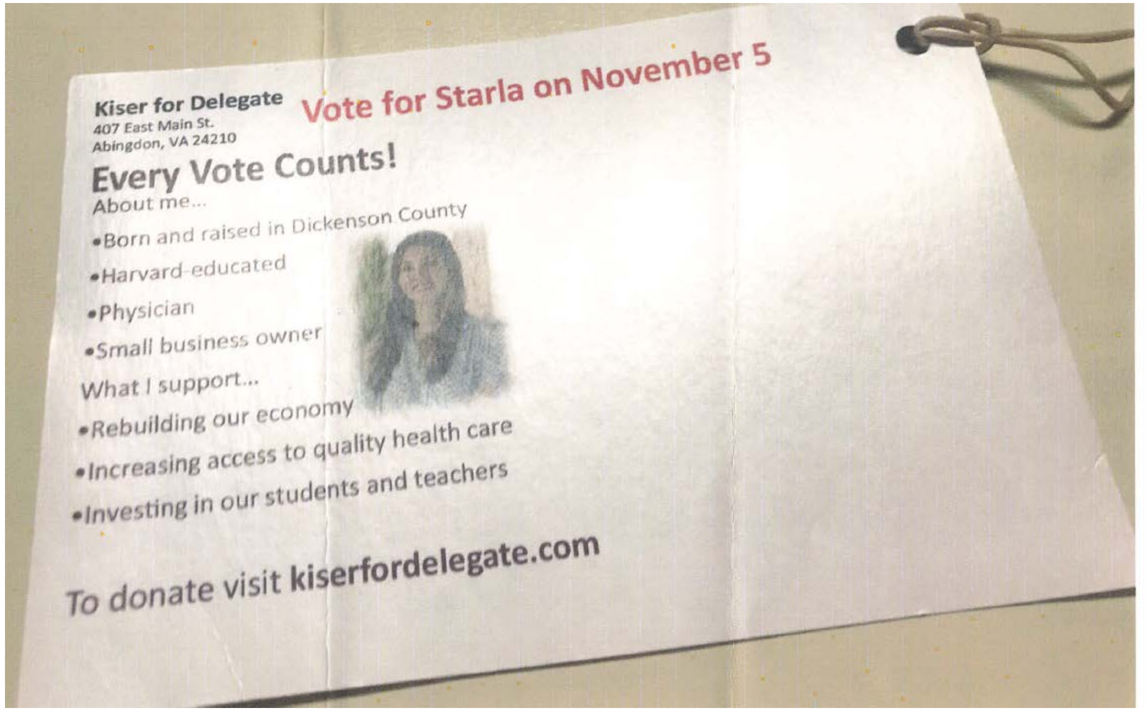
ON AND ABOUT OCTOBER 24, 2019
ALONG JEFFERSON PARK AVENUE STARTING
NEAR FONTAINE + MAURY INTERSECTION IN
CHARLOTTESVILE, VA, AND ALSO ALONG EMMET
STREET.

17. Kiser for Delegate CC-19-00739

1 door tag

Anonymous





Kiser for Delegate
407 East Main St.
Abingdon, VA 24210

Vote for Starla on November 5

Every Vote Counts!

About me...

- Born and raised in Dickenson County
- Harvard-educated
- Physician
- Small business owner

What I support...

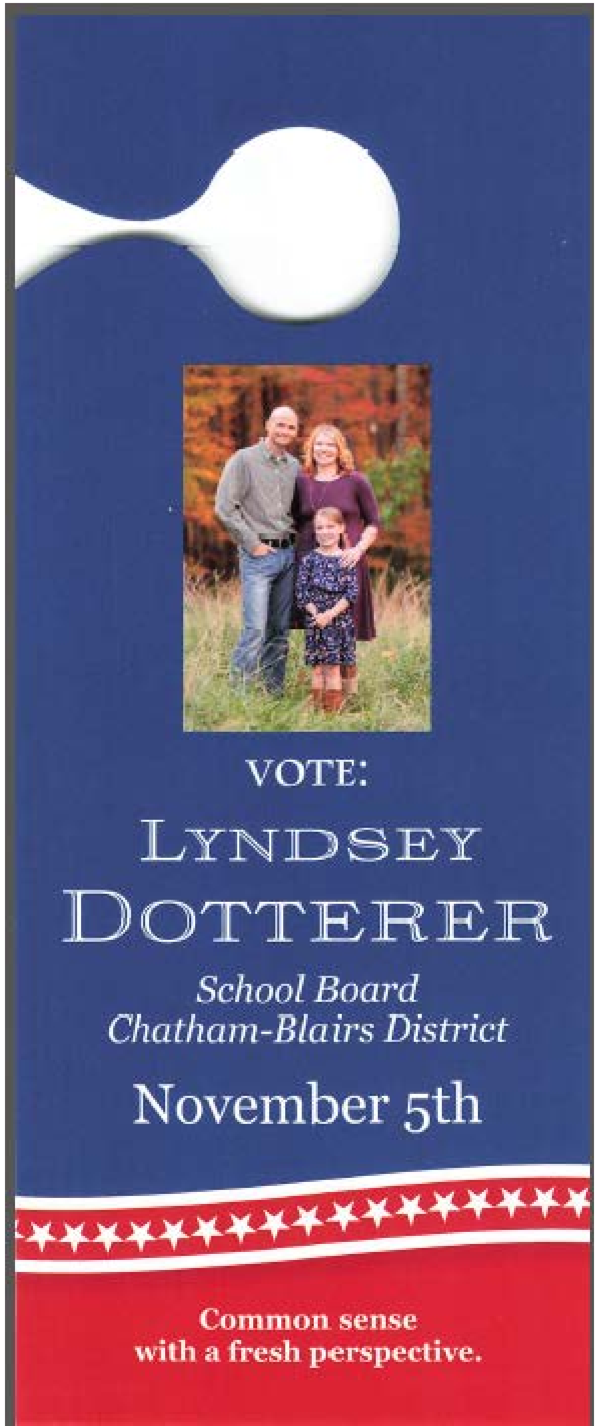
- Rebuilding our economy
- Increasing access to quality health care
- Investing in our students and teachers

To donate visit kiserfordelegate.com

Tell us WHERE and WHEN you saw the ad(s). *Add additional pages if needed.*

The attached flyer which lacked the proper disclaimer was distributed in the following places on the following dates: on July 4, 2019 in Clintwood, Virginia to several hundred people;
on July 4, 2019 in Lebanon, Virginia to several hundred people;
on August 18, 2019 in Washington County, Virginia to a number of residents by the candidate and volunteers;
on August 22, 2019 in Abingdon, Virginia.

18. Lyndsey Dotterer



VOTE:

LYNDSEY DOTTERER

School Board
Chatham-Blairs District

November 5th

Common sense
with a fresh perspective.

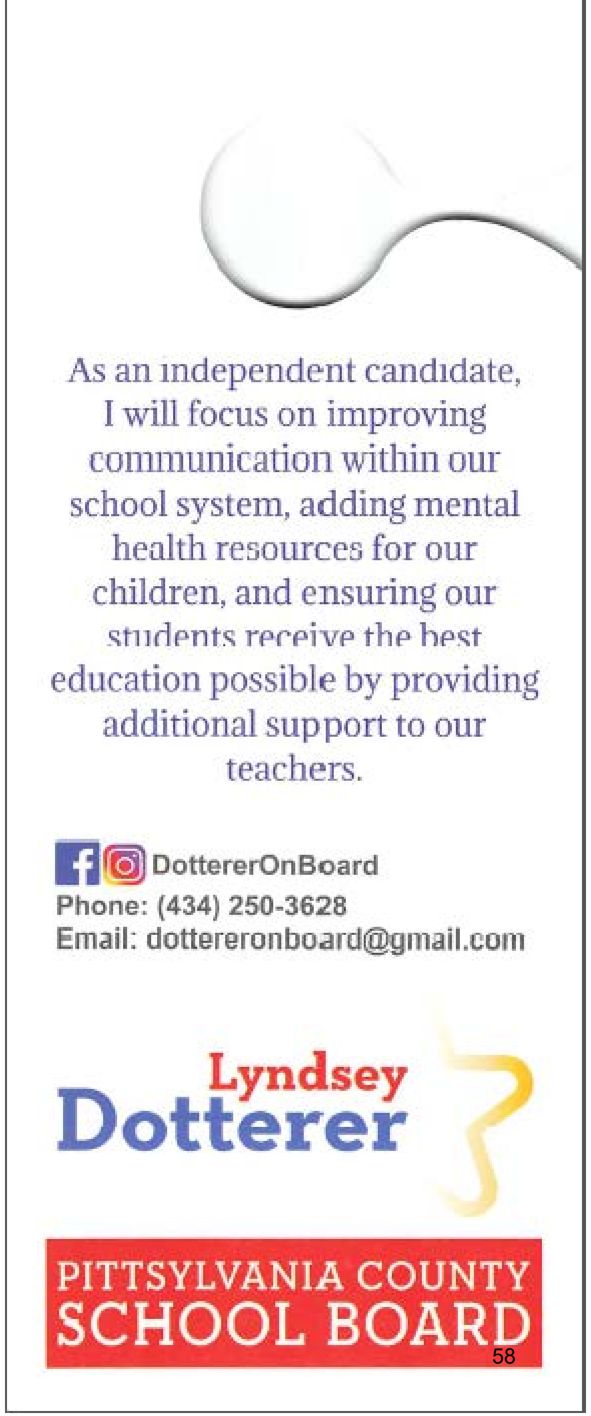
Tell us WHERE and WHEN you saw the ad(s). *Add additional pages if needed.*

Lyndsey Dotterer for School Board door hanger with no campaign disclaimer found in front of my house on October 13.

John Doe
P.O. Box 212
Chatham, VA 24531

1 door hanger

Complaint by "John Doe"



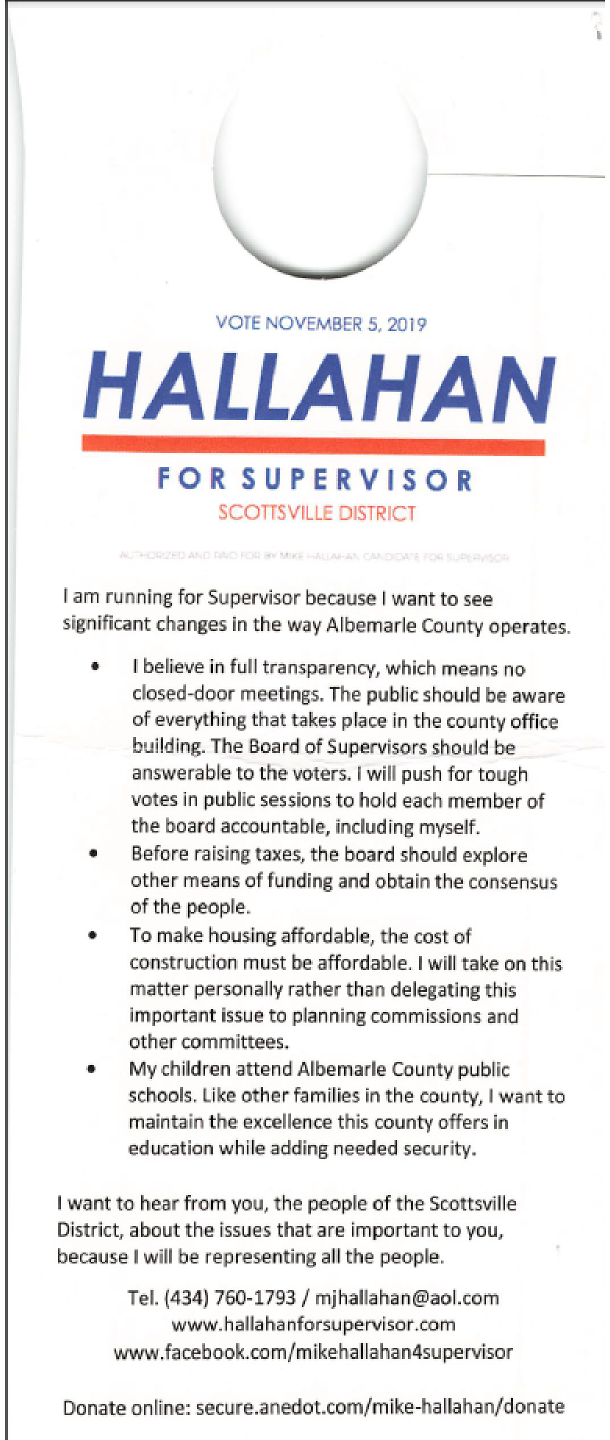
As an independent candidate, I will focus on improving communication within our school system, adding mental health resources for our children, and ensuring our students receive the best education possible by providing additional support to our teachers.

DottererOnBoard
Phone: (434) 250-3628
Email: dottereronboard@gmail.com

Lyndsey Dotterer

PITTSYLVANIA COUNTY
SCHOOL BOARD

19. Michael J. Hallahan, II –Candidate for Supervisor CC-19-00259



VOTE NOVEMBER 5, 2019

HALLAHAN

FOR SUPERVISOR

SCOTTSVILLE DISTRICT

AUTHORIZED AND PAID FOR BY MIKE HALLAHAN CANDIDATE FOR SUPERVISOR

I am running for Supervisor because I want to see significant changes in the way Albemarle County operates.

- I believe in full transparency, which means no closed-door meetings. The public should be aware of everything that takes place in the county office building. The Board of Supervisors should be answerable to the voters. I will push for tough votes in public sessions to hold each member of the board accountable, including myself.
- Before raising taxes, the board should explore other means of funding and obtain the consensus of the people.
- To make housing affordable, the cost of construction must be affordable. I will take on this matter personally rather than delegating this important issue to planning commissions and other committees.
- My children attend Albemarle County public schools. Like other families in the county, I want to maintain the excellence this county offers in education while adding needed security.

I want to hear from you, the people of the Scottsville District, about the issues that are important to you, because I will be representing all the people.

Tel. (434) 760-1793 / mjhallahan@aol.com
www.hallahanforsupervisor.com
www.facebook.com/mikehallahan4supervisor

Donate online: secure.anedot.com/mike-hallahan/donate

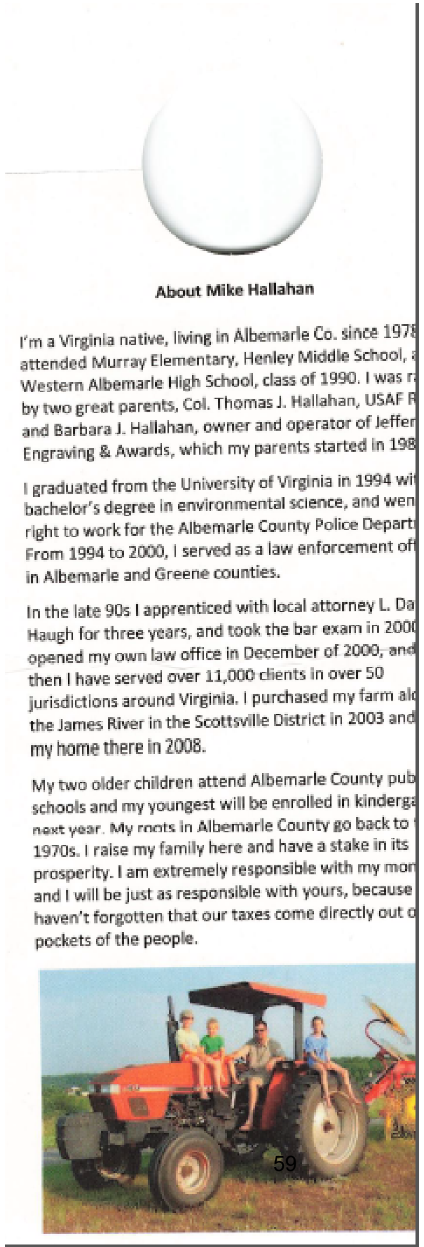
1 door hanger

Anonymous

. Tell us WHERE and WHEN you saw the ad(s). *Add additional pages if needed.*

Handed out in Scottsville, around the time of the
Batteau Fest (June 2019).

"Paid for" disclaimer is not at least 7pt type.



About Mike Hallahan

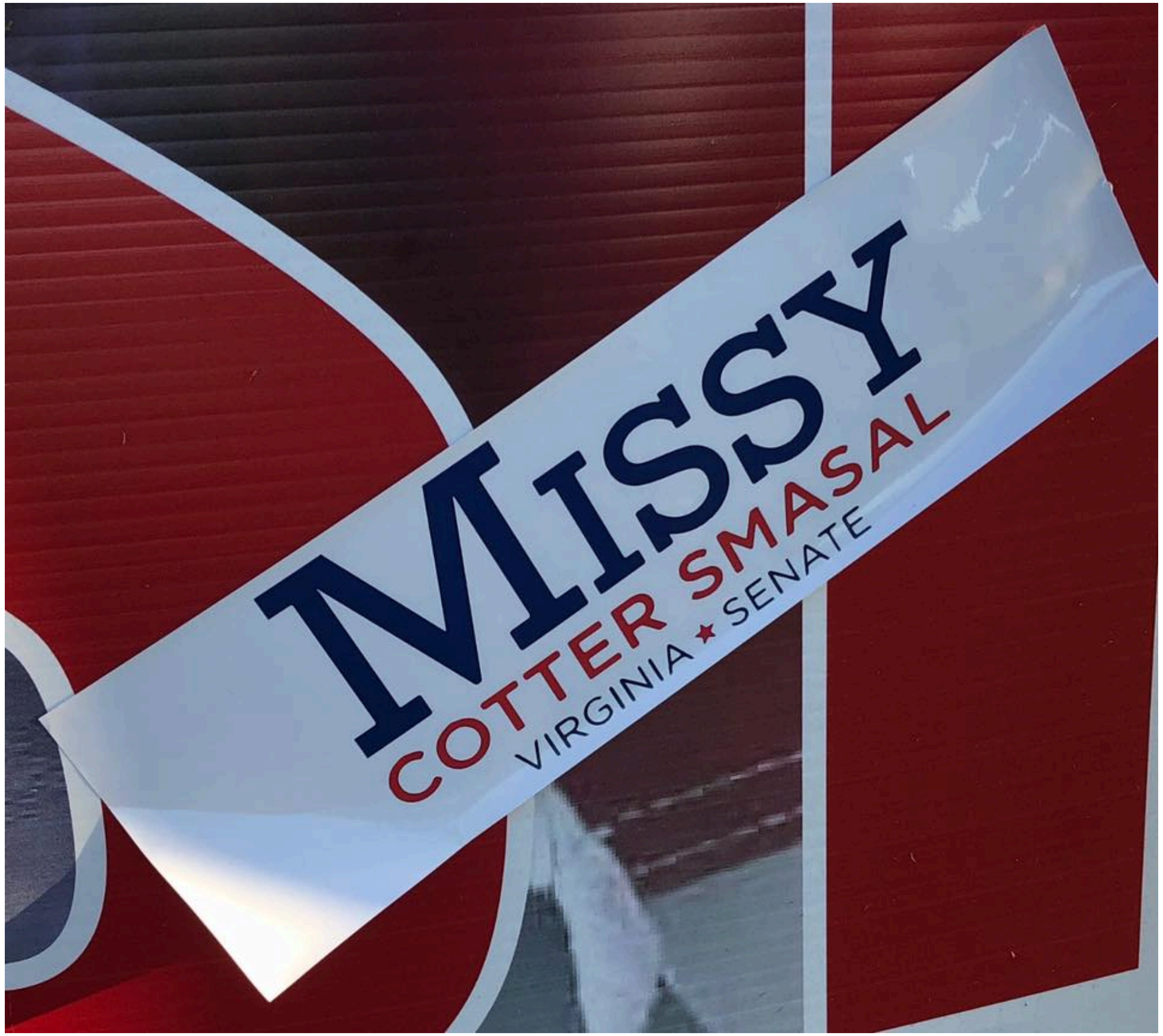
I'm a Virginia native, living in Albemarle Co. since 1978
attended Murray Elementary, Henley Middle School, a
Western Albemarle High School, class of 1990. I was ra
by two great parents, Col. Thomas J. Hallahan, USAF R
and Barbara J. Hallahan, owner and operator of Jeffer
Engraving & Awards, which my parents started in 198

I graduated from the University of Virginia in 1994 wi
bachelor's degree in environmental science, and wen
right to work for the Albemarle County Police Depart
From 1994 to 2000, I served as a law enforcement off
in Albemarle and Greene counties.

In the late 90s I apprenticed with local attorney L. Da
Haugh for three years, and took the bar exam in 2000
opened my own law office in December of 2000, and
then I have served over 11,000 clients in over 50
jurisdictions around Virginia. I purchased my farm alo
the James River in the Scottsville District in 2003 and
my home there in 2008.

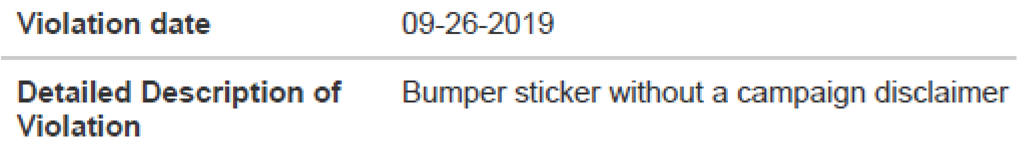
My two older children attend Albemarle County pub
schools and my youngest will be enrolled in kinderga
next year. My roots in Albemarle County go back to t
1970s. I raise my family here and have a stake in its
prosperity. I am extremely responsible with my mon
and I will be just as responsible with yours, because
haven't forgotten that our taxes come directly out o
pockets of the people.

20. Missy for Senate CC-18-00546



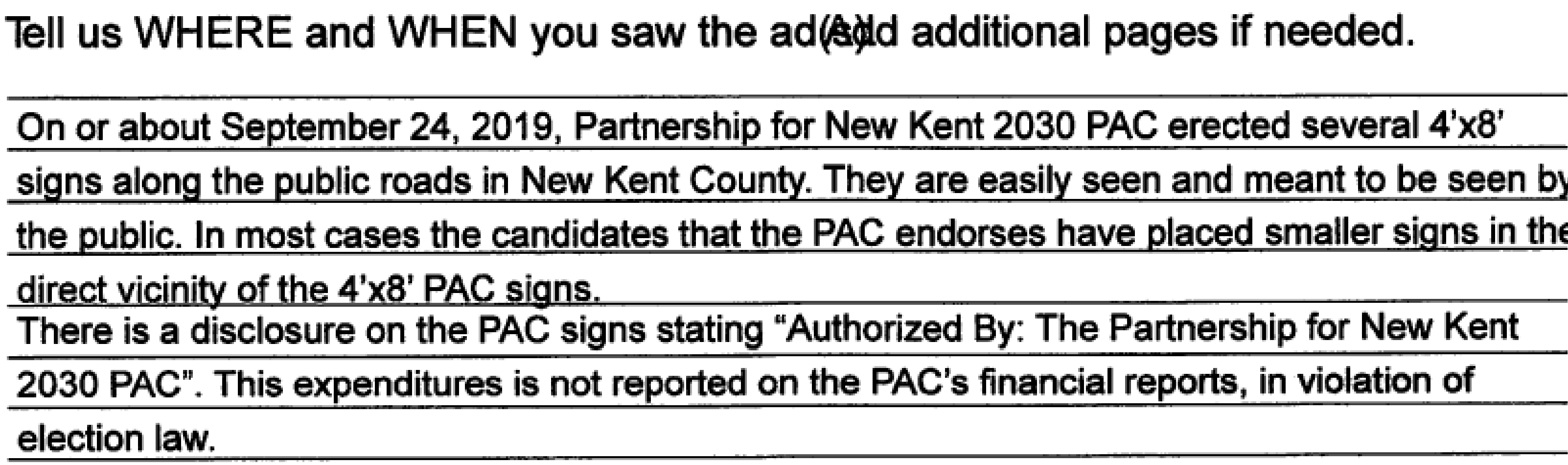
1 bumper sticker

Complaint by Brian Kirwin



Violation date	09-26-2019
Detailed Description of Violation	Bumper sticker without a campaign disclaimer

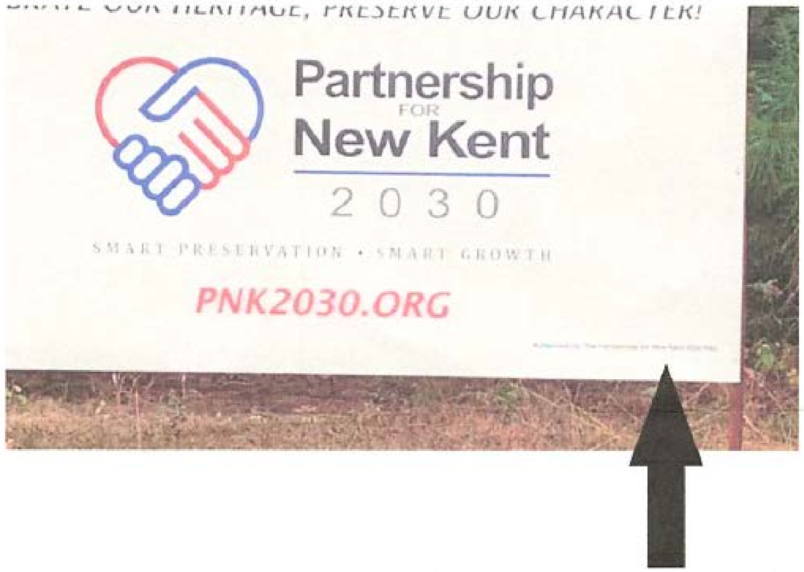
21. Partnership for New Kent 2030 Political Action Committee PAC-19-01032



Tell us WHERE and WHEN you saw the ad(s)Add additional pages if needed.

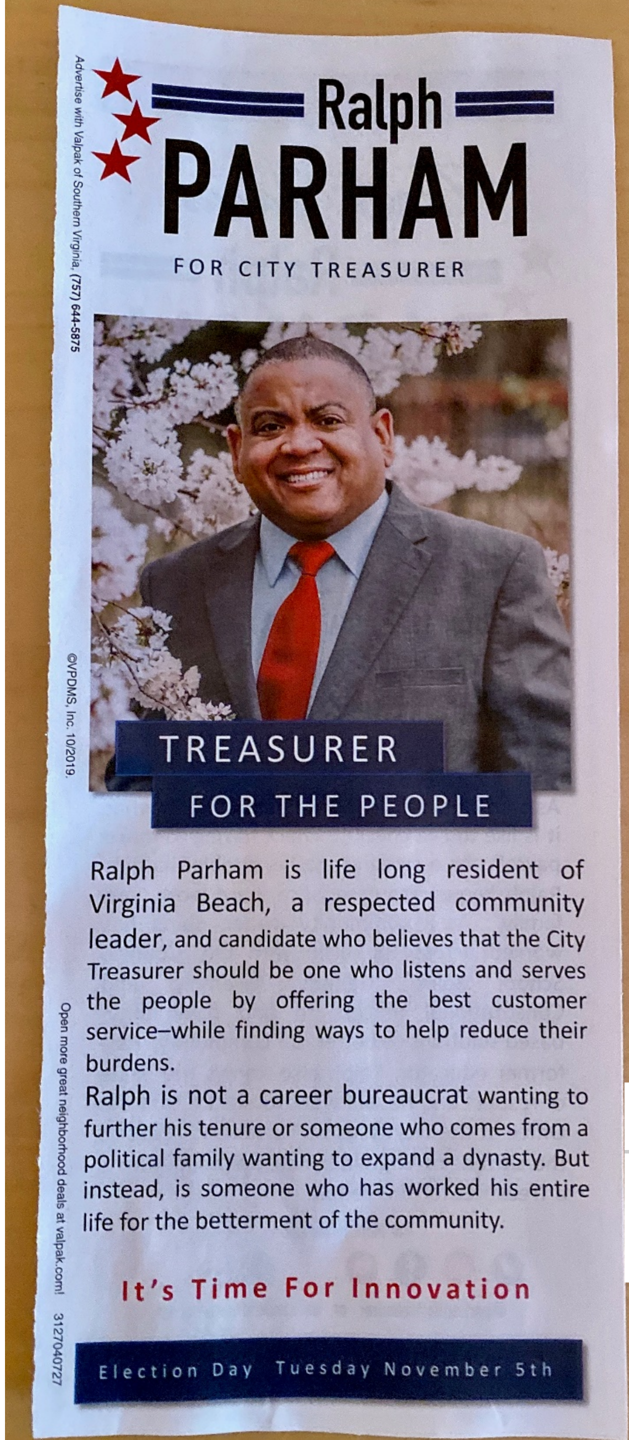
On or about September 24, 2019, Partnership for New Kent 2030 PAC erected several 4'x8' signs along the public roads in New Kent County. They are easily seen and meant to be seen by the public. In most cases the candidates that the PAC endorses have placed smaller signs in the direct vicinity of the 4'x8' PAC signs.

There is a disclosure on the PAC signs stating "Authorized By: The Partnership for New Kent 2030 PAC". This expenditures is not reported on the PAC's financial reports, in violation of election law.


OUR HERITAGE, PRESERVE OUR CHARACTER!
Partnership FOR New Kent
2030
SMART PRESERVATION • SMART GROWTH
PNK2030.ORG

"Authorized by: The Partnership for New Kent 2030 PAC"

22. Ralph Parham for Treasurer CC-19-00199



Ralph Parham is life long resident of Virginia Beach, a respected community leader, and candidate who believes that the City Treasurer should be one who listens and serves the people by offering the best customer service–while finding ways to help reduce their burdens.

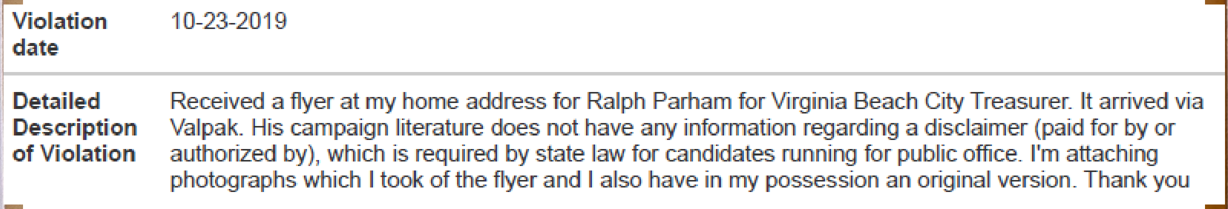
Ralph is not a career bureaucrat wanting to further his tenure or someone who comes from a political family wanting to expand a dynasty. But instead, is someone who has worked his entire life for the betterment of the community.

It's Time For Innovation

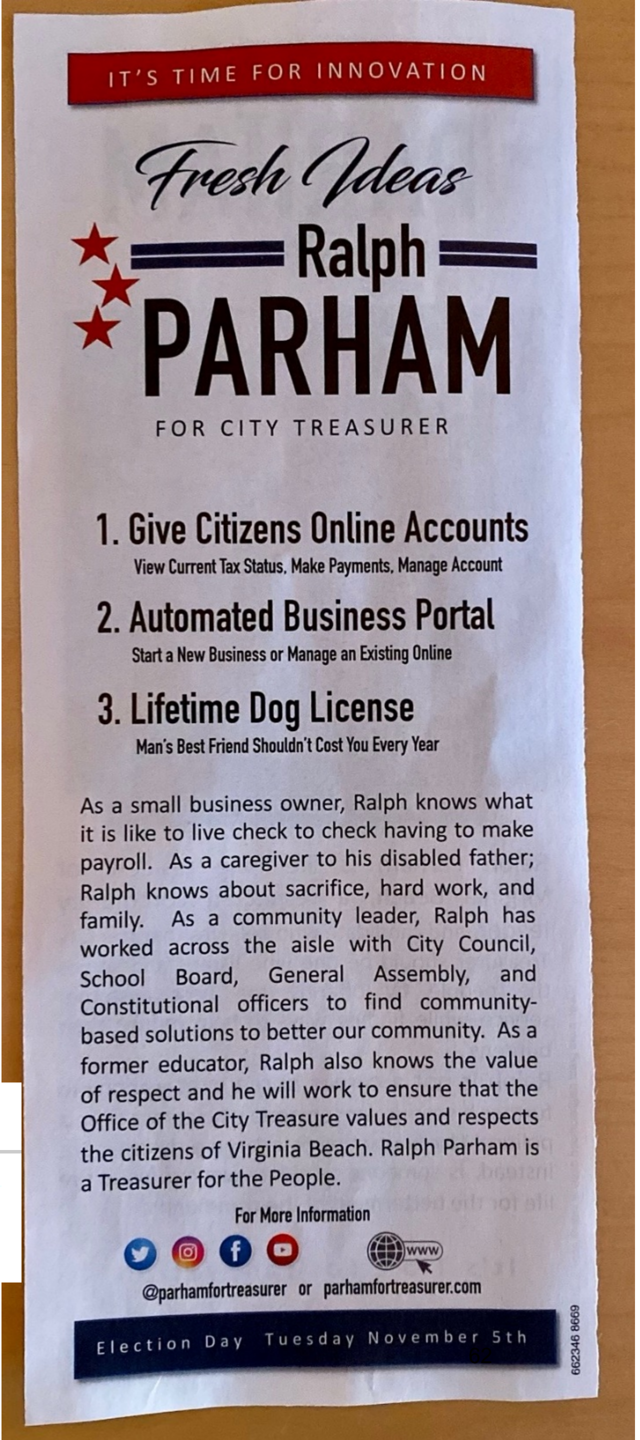
Election Day Tuesday November 5th

1 Val-Pak Insert

Online Complaint by Lisa Turner



Violation date	10-23-2019
Detailed Description of Violation	Received a flyer at my home address for Ralph Parham for Virginia Beach City Treasurer. It arrived via Valpak. His campaign literature does not have any information regarding a disclaimer (paid for by or authorized by), which is required by state law for candidates running for public office. I'm attaching photographs which I took of the flyer and I also have in my possession an original version. Thank you



IT'S TIME FOR INNOVATION

1. Give Citizens Online Accounts
View Current Tax Status, Make Payments, Manage Account
2. Automated Business Portal
Start a New Business or Manage an Existing Online
3. Lifetime Dog License
Man's Best Friend Shouldn't Cost You Every Year

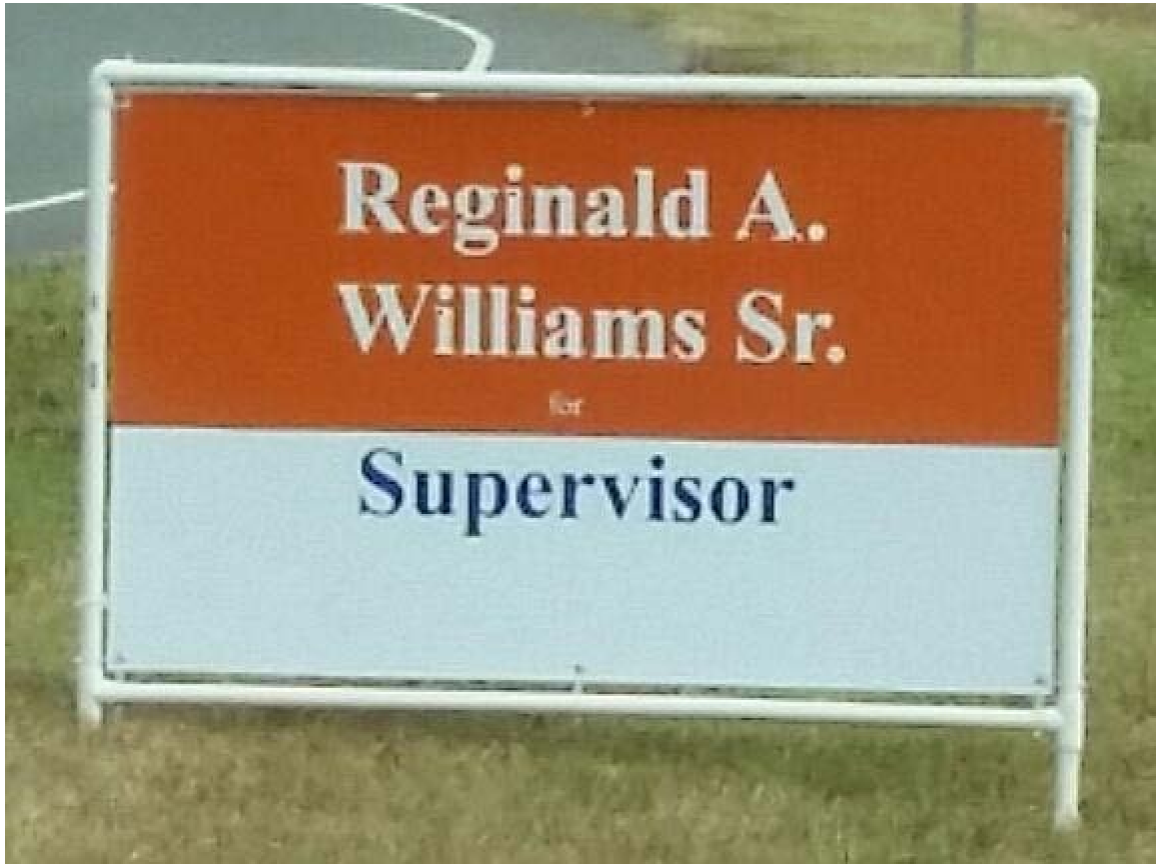
As a small business owner, Ralph knows what it is like to live check to check having to make payroll. As a caregiver to his disabled father; Ralph knows about sacrifice, hard work, and family. As a community leader, Ralph has worked across the aisle with City Council, School Board, General Assembly, and Constitutional officers to find community-based solutions to better our community. As a former educator, Ralph also knows the value of respect and he will work to ensure that the Office of the City Treasure values and respects the citizens of Virginia Beach. Ralph Parham is a Treasurer for the People.

For More Information

@parhamfortreasurer or parhamfortreasurer.com

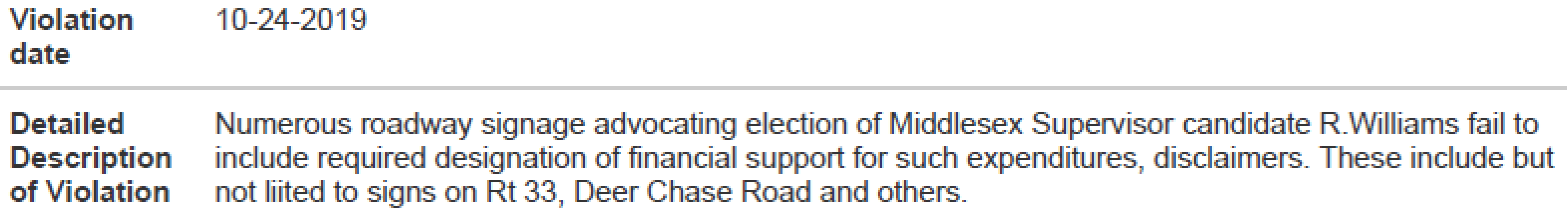
Election Day Tuesday November 5th

23. Reginald A. Williams, Sr.



One Sign

Online Complaint by Harry Roden



Violation date	10-24-2019
Detailed Description of Violation	Numerous roadway signage advocating election of Middlesex Supervisor candidate R.Williams fail to include required designation of financial support for such expenditures, disclaimers. These include but not liited to signs on Rt 33, Deer Chase Road and others.

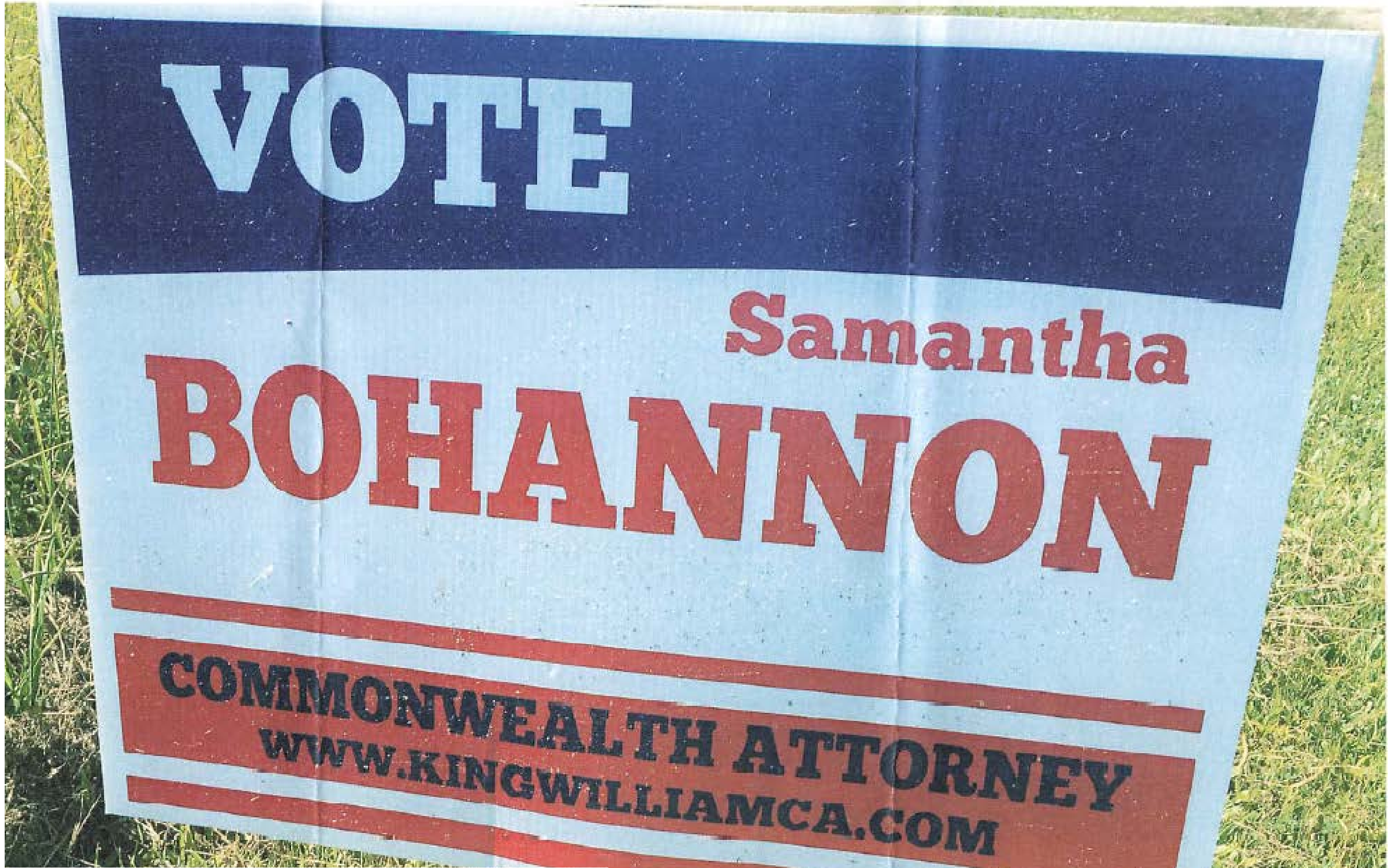
24. Samantha Bohannon, Candidate CC-19-01091

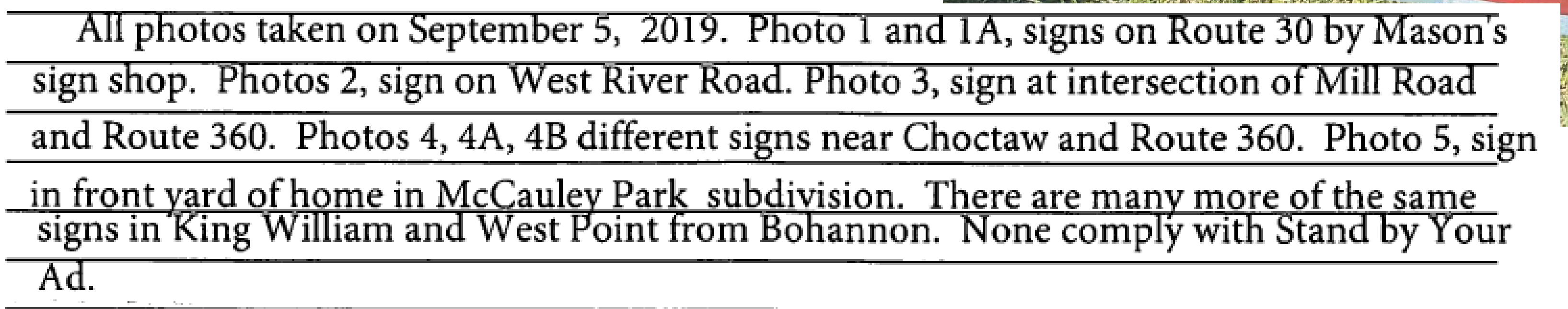
Anonymous Complaint sent via USPS

Violation Date September 5, 2019

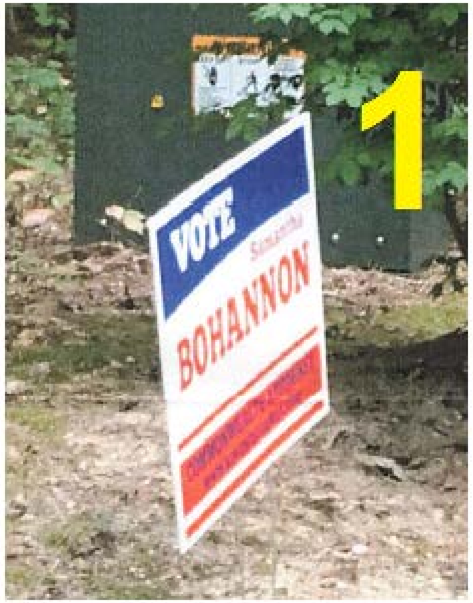
One (1) clear sign

Nine (9) additional signs blurry and/or taken from a distance

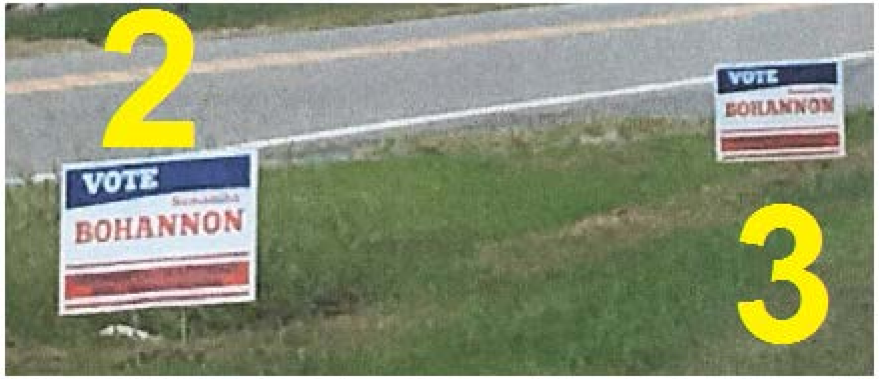


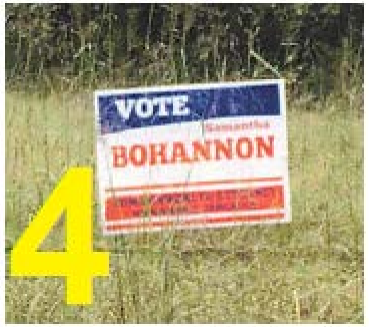


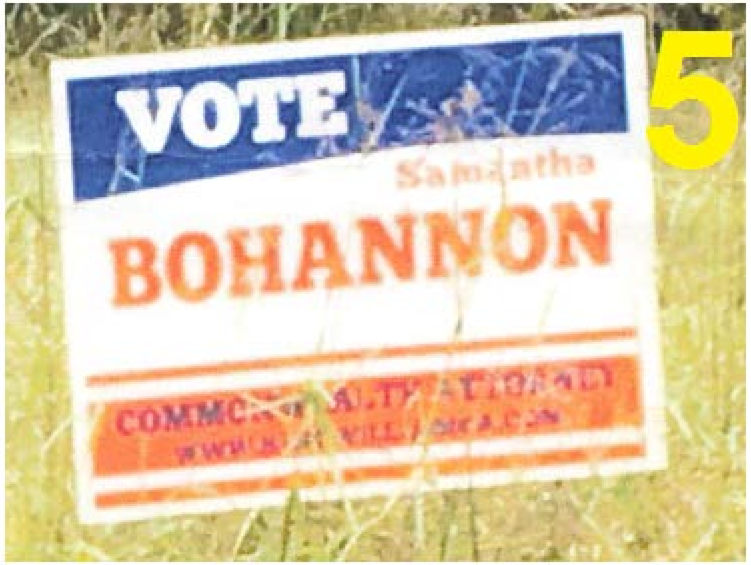
All photos taken on September 5, 2019. Photo 1 and 1A, signs on Route 30 by Mason's sign shop. Photos 2, sign on West River Road. Photo 3, sign at intersection of Mill Road and Route 360. Photos 4, 4A, 4B different signs near Choctaw and Route 360. Photo 5, sign in front yard of home in McCauley Park subdivision. There are many more of the same signs in King William and West Point from Bohannon. None comply with Stand by Your Ad.

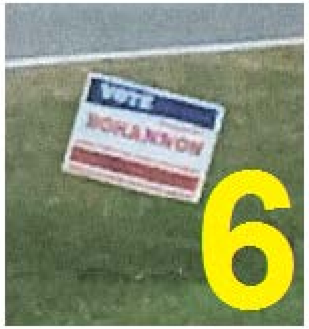


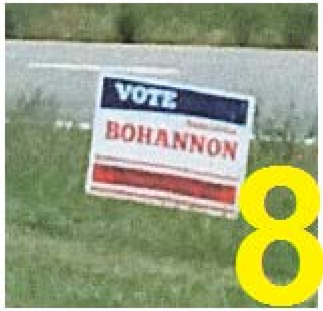
Nine (9) additional signs presented as they were received by ELECT

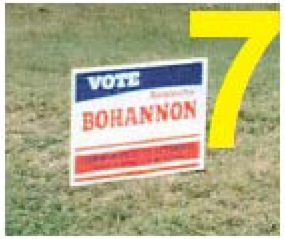


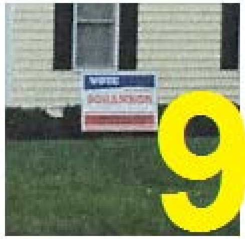










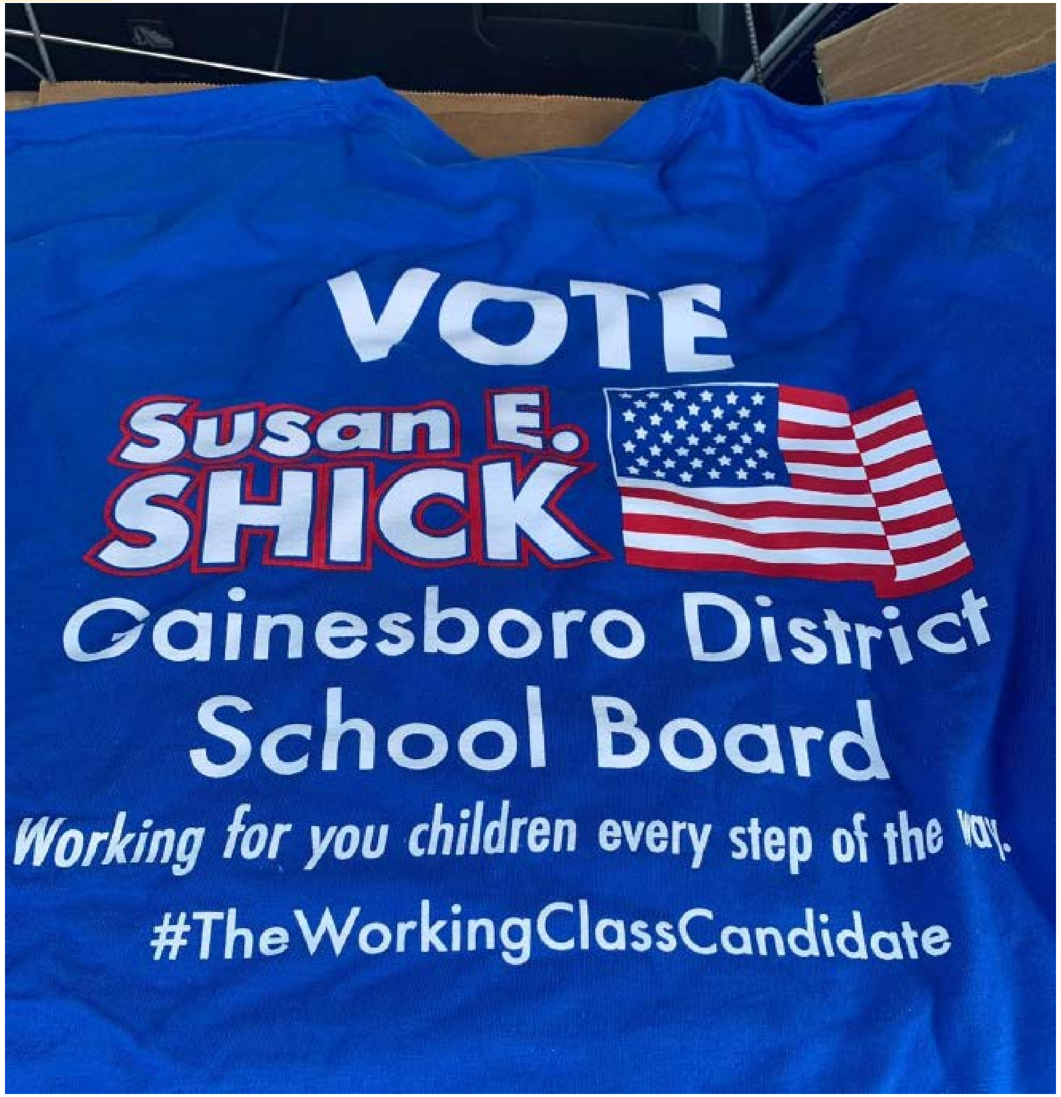


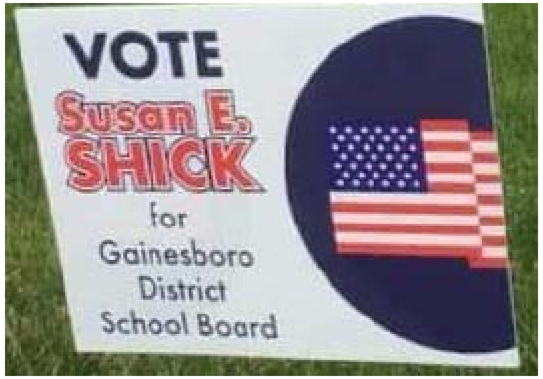
25. Shick for Gainesboro District School Board CC-CC-19-00724

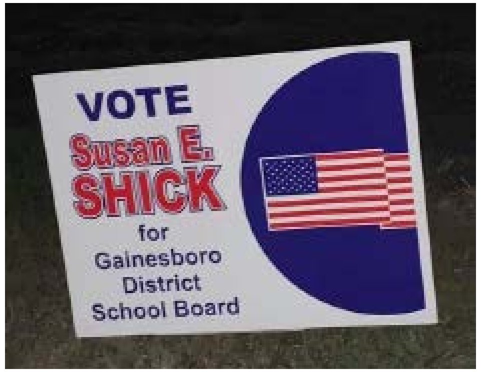
Complaint by Nancy DeZarn via online complaint form

1 T-shirt, 2 signs

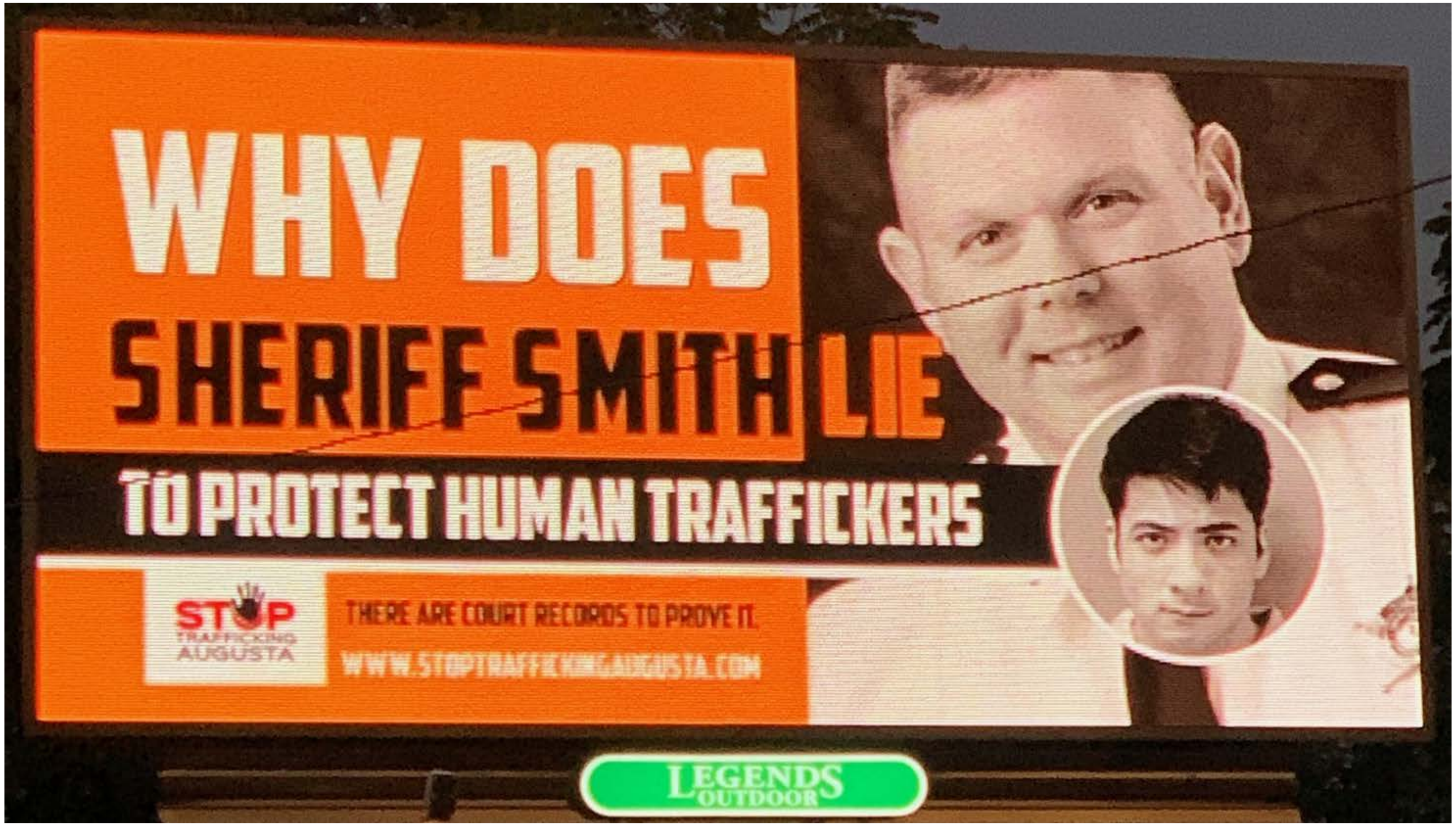
Violation date 09-30-2019

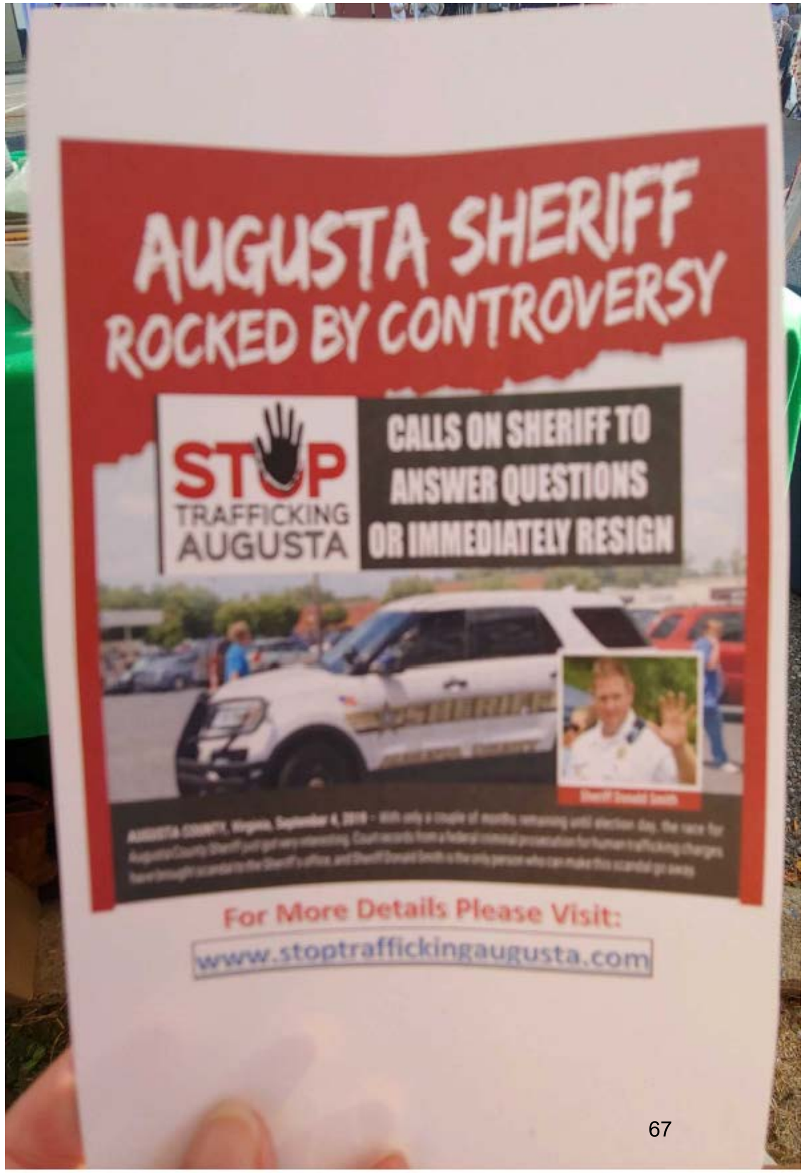

VOTE
Susan E.
SHICK
Gainesboro District
School Board
Working for you children every step of the way.
#TheWorkingClassCandidate





26. Stop Trafficking Augusta PAC-19-01040


WHY DOES
SHERIFF SMITH LIE
TO PROTECT HUMAN TRAFFICKERS
STOP TRAFFICKING AUGUSTA
THERE ARE COURT RECORDS TO PROVE IT.
WWW.STOPTRAFFICKINGAUGUSTA.COM
LEGENDS OUTDOOR



AUGUSTA COUNTY, Virginia, September 4, 2019 – With only a couple of months remaining until election day, the race for Augusta County Sheriff just got very interesting. Court records from a federal criminal prosecution for human trafficking charges have brought scandal to the Sheriff's office, and Sheriff Donald Smith is the only person who can make this scandal go away.

For More Details Please Visit:
www.stoptraffickingaugusta.com

1 billboard , 1 flyer

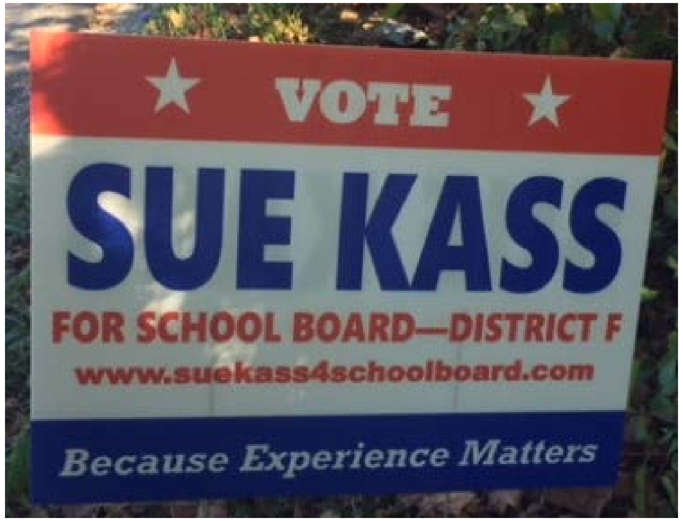
Online complaint by
Donald Smith

27. Sue Kass for School Board CC-19-00933

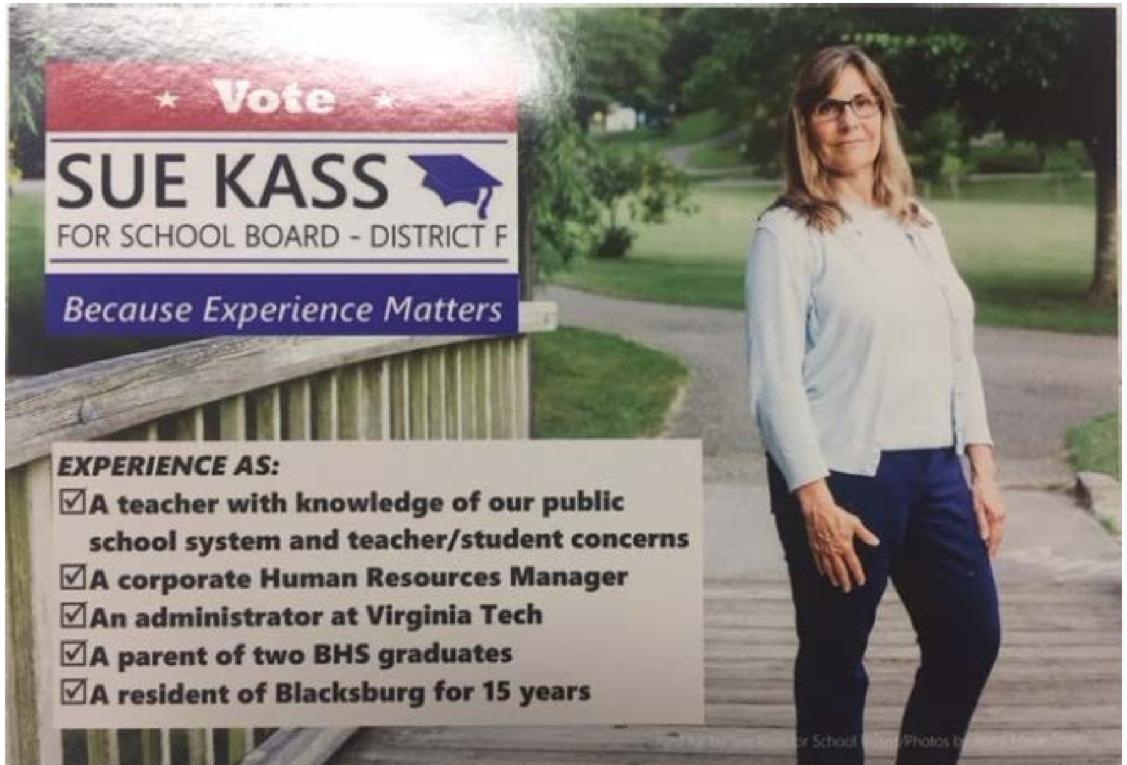
1 sign, 1 card (both front and back)

Online complaint from Sofia Midkiff

Violation date	07-25-2019


★ VOTE ★
SUE KASS
FOR SCHOOL BOARD—DISTRICT F
www.suekass4schoolboard.com
Because Experience Matters

★ VOTE ★
SUE KASS
FOR SCHOOL BOARD—DISTRICT F
www.suekass4schoolboard.com
Because Experience Matters



EXPERIENCE AS:

☑A teacher with knowledge of our public school system and teacher/student concerns

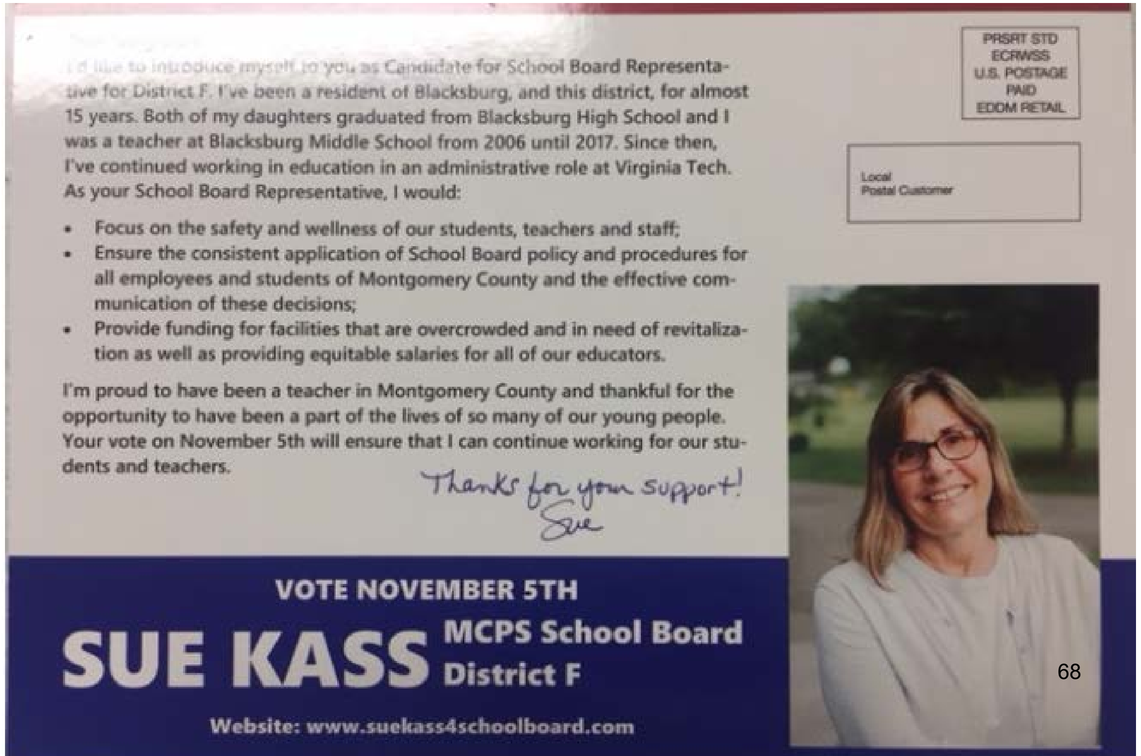
☑A corporate Human Resources Manager

☑An administrator at Virginia Tech

☑A parent of two BHS graduates

☑A resident of Blacksburg for 15 years

Paid for by Sue Kass for School Board/Photos by [illegible]



I'd like to introduce myself to you as Candidate for School Board Representative for District F. I've been a resident of Blacksburg, and this district, for almost 15 years. Both of my daughters graduated from Blacksburg High School and I was a teacher at Blacksburg Middle School from 2006 until 2017. Since then, I've continued working in education in an administrative role at Virginia Tech. As your School Board Representative, I would:

- Focus on the safety and wellness of our students, teachers and staff;
- Ensure the consistent application of School Board policy and procedures for all employees and students of Montgomery County and the effective communication of these decisions;
- Provide funding for facilities that are overcrowded and in need of revitalization as well as providing equitable salaries for all of our educators.

I'm proud to have been a teacher in Montgomery County and thankful for the opportunity to have been a part of the lives of so many of our young people. Your vote on November 5th will ensure that I can continue working for our students and teachers.

Thanks for your support!
Sue

PRSRT STD
ECRWSS
U.S. POSTAGE
PAID
EDDM RETAIL

Local
Postal Customer

VOTE NOVEMBER 5TH

SUE KASS MCPS School Board District F

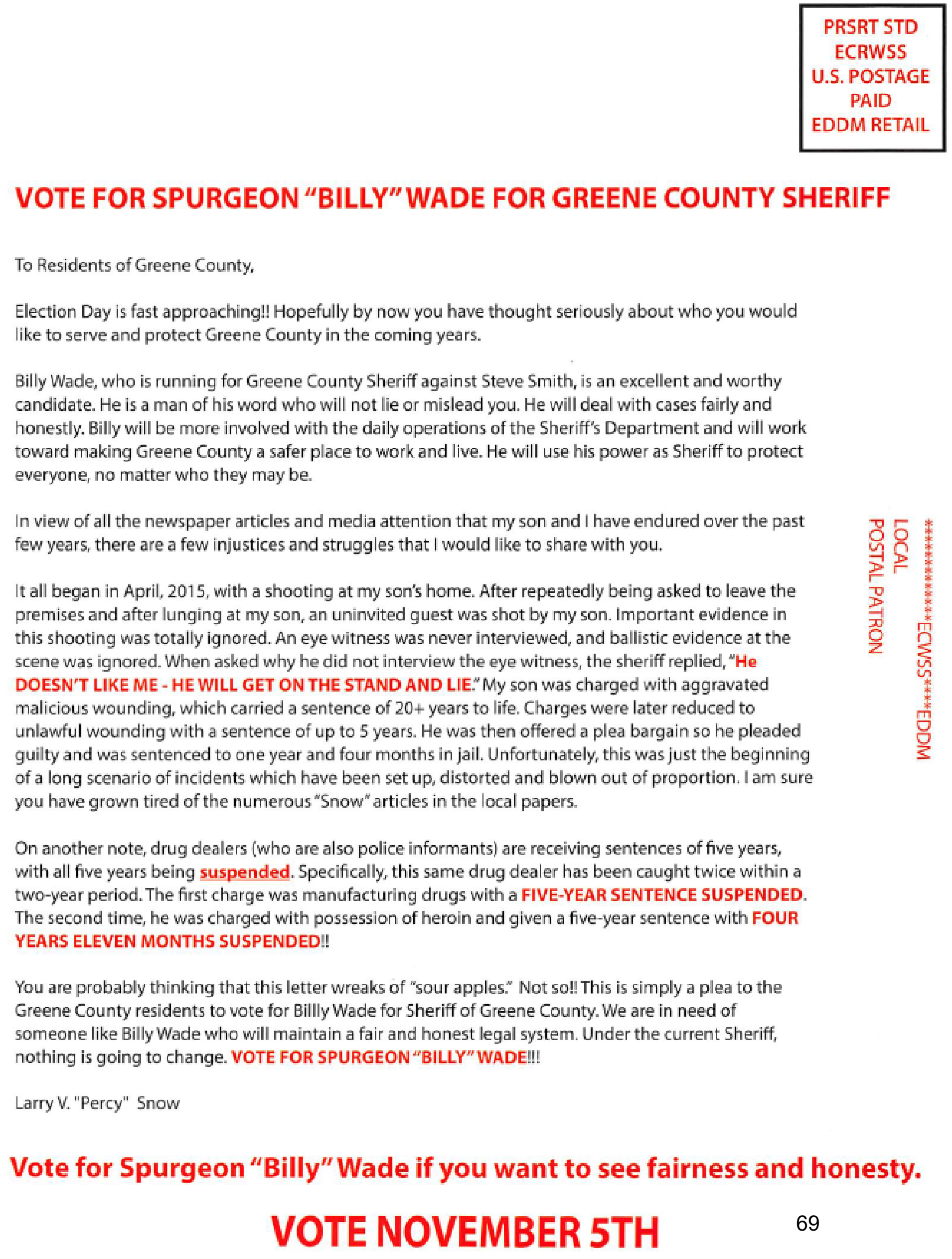
Website: www.suekass4schoolboard.com

28. Wade for Sheriff. CC-19-00844

1 mass mailer, one side only

Online complaint by Steve Smith

Violation date	10-30-2019
Detailed Description of Violation	No disclaimer on mass mailer



PRSRT STD
ECRWSS
U.S. POSTAGE
PAID
EDDM RETAIL

VOTE FOR SPURGEON "BILLY" WADE FOR GREENE COUNTY SHERIFF

To Residents of Greene County,

Election Day is fast approaching!! Hopefully by now you have thought seriously about who you would like to serve and protect Greene County in the coming years.

Billy Wade, who is running for Greene County Sheriff against Steve Smith, is an excellent and worthy candidate. He is a man of his word who will not lie or mislead you. He will deal with cases fairly and honestly. Billy will be more involved with the daily operations of the Sheriff's Department and will work toward making Greene County a safer place to work and live. He will use his power as Sheriff to protect everyone, no matter who they may be.

In view of all the newspaper articles and media attention that my son and I have endured over the past few years, there are a few injustices and struggles that I would like to share with you.

It all began in April, 2015, with a shooting at my son's home. After repeatedly being asked to leave the premises and after lunging at my son, an uninvited guest was shot by my son. Important evidence in this shooting was totally ignored. An eye witness was never interviewed, and ballistic evidence at the scene was ignored. When asked why he did not interview the eye witness, the sheriff replied, "**He DOESN'T LIKE ME - HE WILL GET ON THE STAND AND LIE.**" My son was charged with aggravated malicious wounding, which carried a sentence of 20+ years to life. Charges were later reduced to unlawful wounding with a sentence of up to 5 years. He was then offered a plea bargain so he pleaded guilty and was sentenced to one year and four months in jail. Unfortunately, this was just the beginning of a long scenario of incidents which have been set up, distorted and blown out of proportion. I am sure you have grown tired of the numerous "Snow" articles in the local papers.

On another note, drug dealers (who are also police informants) are receiving sentences of five years, with all five years being **suspended**. Specifically, this same drug dealer has been caught twice within a two-year period. The first charge was manufacturing drugs with a **FIVE-YEAR SENTENCE SUSPENDED**. The second time, he was charged with possession of heroin and given a five-year sentence with **FOUR YEARS ELEVEN MONTHS SUSPENDED**!!

You are probably thinking that this letter wreaks of "sour apples." Not so!! This is simply a plea to the Greene County residents to vote for Billly Wade for Sheriff of Greene County. We are in need of someone like Billy Wade who will maintain a fair and honest legal system. Under the current Sheriff, nothing is going to change. **VOTE FOR SPURGEON "BILLY" WADE**!!!

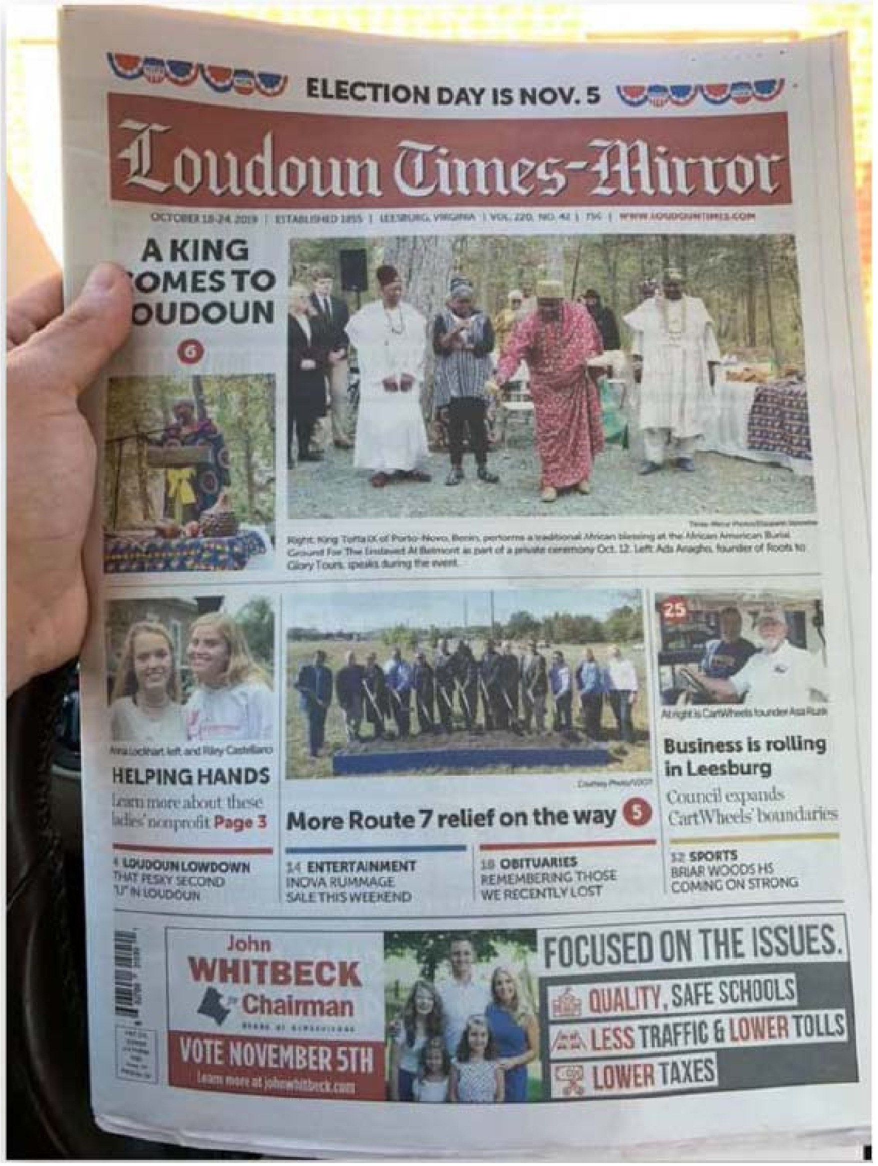
Larry V. "Percy" Snow

Vote for Spurgeon "Billy" Wade if you want to see fairness and honesty.

VOTE NOVEMBER 5TH

************ECWSS****EDDM
LOCAL
POSTAL PATRON

29. Whitbeck for Chairman CC-19-0174



ELECTION DAY IS NOV. 5

Loudoun Times-Mirror

OCTOBER 18-24, 2019 | ESTABLISHED 1855 | LEESBURG, VIRGINIA | VOL. 220, NO. 42 | 75¢ | WWW.LOUDOUNTIMES.COM

A KING COMES TO LOUDOUN 6

Right: King Tofta IX of Porto-Novo, Benin, performs a traditional African blessing at the African American Burial Ground For The Enslaved At Belmont as part of a private ceremony Oct. 12. Left: Ada Aragho, founder of Roots to Glory Tours, speaks during the event.

Ana Lockhart, left, and Riley Castellano

HELPING HANDS

Learn more about these ladies' nonprofit Page 3

More Route 7 relief on the way 5

25

At right is CartWheels founder Asa Rush

Business is rolling in Leesburg

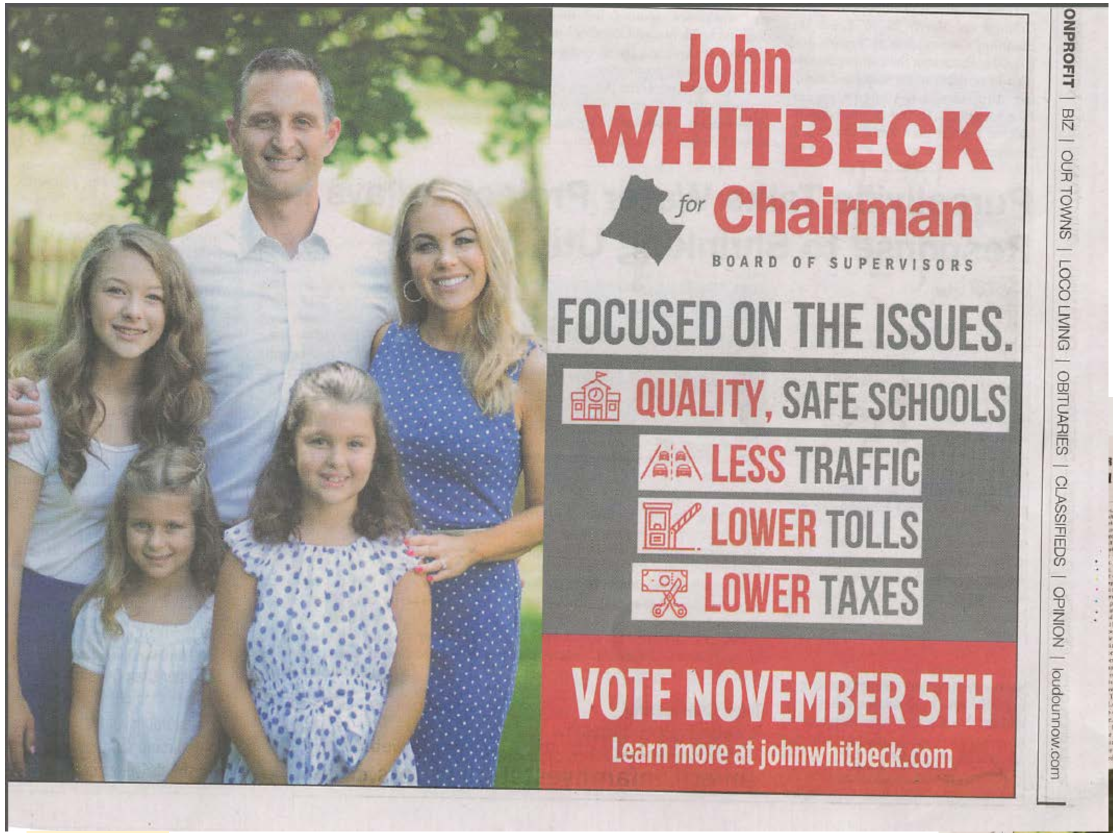
Council expands CartWheels' boundaries

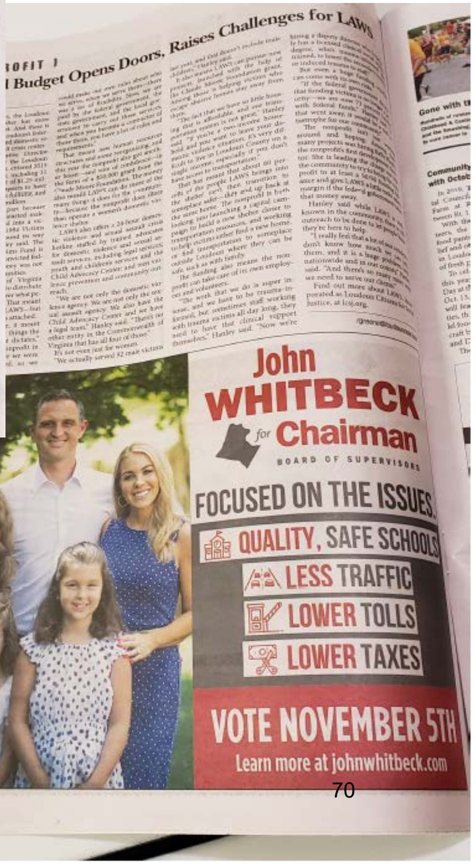
4 LOUDOUN LOWDOWN THAT PESKY SECOND "U" IN LOUDOUN

14 ENTERTAINMENT INOVA RUMMAGE SALE THIS WEEKEND

18 OBITUARIES REMEMBERING THOSE WE RECENTLY LOST

32 SPORTS BRIAR WOODS HS COMING ON STRONG





Budget Opens Doors, Raises Challenges for LAWS

3 ads

2 received via online by Joan Kowalski and Charlotte MCConnell

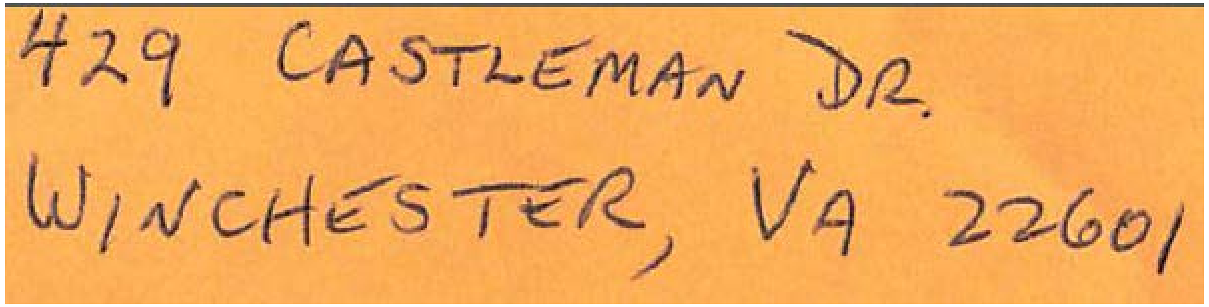
1 entire edition of Loudoun Now

Violation Dates October 17 and 18, 2019

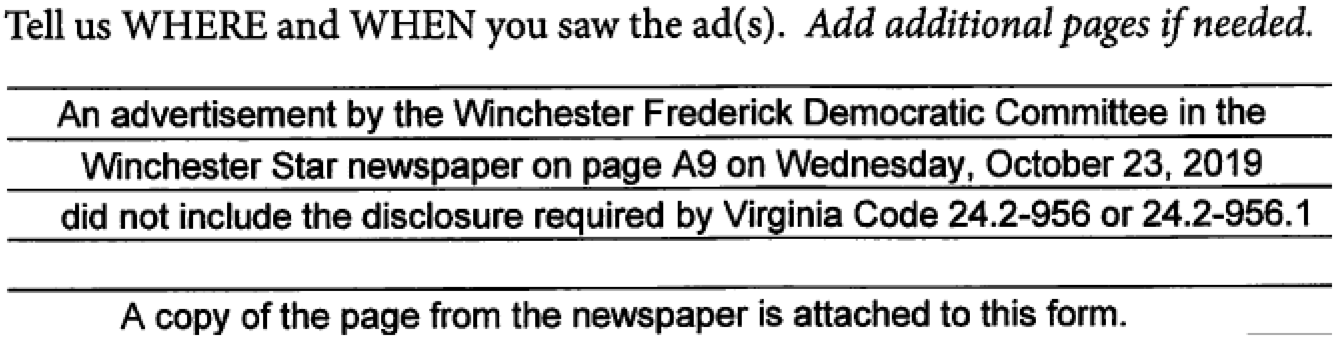
30. Winchester – Frederick Democratic Committee

1 newspaper ad

Anonymous complaint received via snail mail



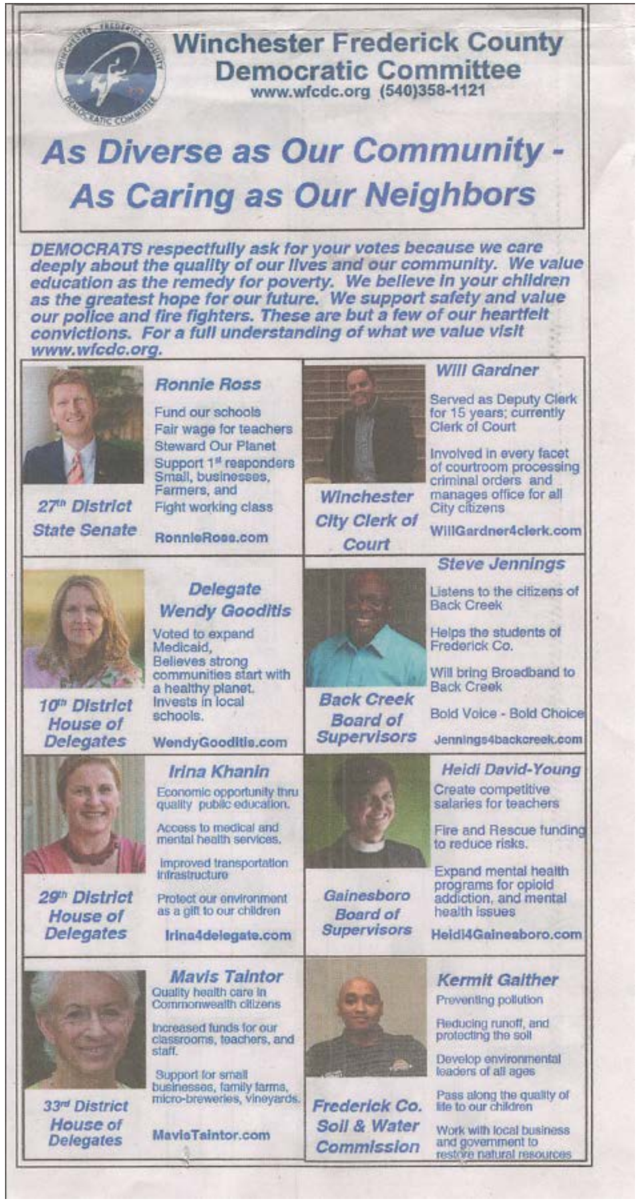
429 CASTLEMAN DR.
WINCHESTER, VA 22601



Tell us WHERE and WHEN you saw the ad(s). *Add additional pages if needed.*

An advertisement by the Winchester Frederick Democratic Committee in the Winchester Star newspaper on page A9 on Wednesday, October 23, 2019 did not include the disclosure required by Virginia Code 24.2-956 or 24.2-956.1

A copy of the page from the newspaper is attached to this form.



**Winchester Frederick County
Democratic Committee**
www.wfcdc.org (540)358-1121

***As Diverse as Our Community -
As Caring as Our Neighbors***

DEMOCRATS respectfully ask for your votes because we care deeply about the quality of our lives and our community. We value education as the remedy for poverty. We believe in your children as the greatest hope for our future. We support safety and value our police and fire fighters. These are but a few of our heartfelt convictions. For a full understanding of what we value visit www.wfcdc.org.

Ronnie Ross

Fund our schools
Fair wage for teachers
Steward Our Planet
Support 1st responders
Small, businesses, Farmers, and
Fight working class

RonnieRoss.com

***27th District
State Senate***

Will Gardner

Served as Deputy Clerk for 15 years; currently Clerk of Court

Involved in every facet of courtroom processing criminal orders and manages office for all City citizens

WillGardner4clerk.com

***Winchester
City Clerk of
Court***

***Delegate
Wendy Gooditis***

Voted to expand Medicaid,
Believes strong communities start with a healthy planet.
Invests in local schools.

WendyGooditis.com

***10th District
House of
Delegates***

Steve Jennings

Listens to the citizens of Back Creek

Helps the students of Frederick Co.

Will bring Broadband to Back Creek

Bold Voice - Bold Choice

Jennings4backcreek.com

***Back Creek
Board of
Supervisors***

Irina Khanin

Economic opportunity thru quality public education.

Access to medical and mental health services.

Improved transportation infrastructure

Protect our environment as a gift to our children

Irina4delegate.com

***29th District
House of
Delegates***

Heidi David-Young

Create competitive salaries for teachers

Fire and Rescue funding to reduce risks.

Expand mental health programs for opioid addiction, and mental health issues

Heidi4Gainesboro.com

***Gainesboro
Board of
Supervisors***

Mavis Taintor

Quality health care in Commonwealth citizens

Increased funds for our classrooms, teachers, and staff.

Support for small businesses, family farms, micro-breweries, vineyards.

MavisTaintor.com

***33rd District
House of
Delegates***

Kermit Gaither

Preventing pollution

Reducing runoff, and protecting the soil

Develop environmental leaders of all ages

Pass along the quality of life to our children

Work with local business and government to restore natural resources

***Frederick Co.
Soil & Water
Commission***

★ VIRGINIA ★
STATE BOARD *of* ELECTIONS

HB2178 Minimum Security Standards

BOARD WORKING PAPERS
Daniel Persico
Chief Information Officer

★ VIRGINIA ★

STATE BOARD *of* ELECTIONS

Memorandum

To: Chairman Brink, Vice Chair O'Bannon, and Secretary LeCruise

From: Dan Persico, Chief Information Officer (CIO)

Date: November 18, 2019

Re: Adoption of remaining HB2178 Minimum Security Standards

Suggested motion for a Board member to make:

Move that the Board adopt the proposed HB2178 minimum security standards related to information systems identified as sensitive to election related activities.

In support of improving elections security maturity within the Commonwealth prior to the 2020 Election, localities are highly encouraged to align their resources to assure that at a minimum, the standards identified with a Risk Priority of critical and high, are implemented by September 1, 2020 – along with any others they believe to be of critical and high risk priority for their locality.

Applicable Code Sections: Va. Code § 24.2-410.2

Attachments:

CONFIDENTIAL – EXEMPT FROM DISTRIBUTION / FOIA per Va. Code § 24.2-625.1 & § 2.2-3705.2(14)

Your Board materials include the following ***confidential (non-FOIA-ble)*** items:

- **20 Minimum Security Standards**: *[Recall Risk Assessment Standard was adopted 9/17]*
  - ✓ Password Management
  - ✓ System & Communications Protection
  - ✓ Incident Response
  - ✓ System & Information Integrity
  - ✓ Security Assessment & Authorization
  - ✓ Awareness and Training
  - ✓ Access Control
  - ✓ Physical Access & Security
  - ✓ Personnel Management
  - ✓ Program Management
  - ✓ Media Protection
  - ✓ Physical and Environmental Protection

- ✓ Security Planning
- ✓ System & Services Acquisition
- ✓ Maintenance
- ✓ Contingency Planning
- ✓ Configuration Management
- ✓ Security & Acceptable Use
- ✓ Audit & Accountability
- ✓ Policies & Procedures

- **Work group General Cost Estimates** (to implement the proposed minimum security standards, and includes a work group determined Risk Priority for each standard; **C**ritical, **H**igh, **M**oderate or **L**ow)

Background:

Pursuant to § 24.2-410.2, the State Board must "promulgate regulations and standards necessary to ensure the security and integrity of the Virginia voter registration system and the supporting technologies…".

Further, "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*."

In alignment, the prescribed work group reviewed the proposed standards and developed General Cost Estimates for implementation of these standards for your review. The General Cost Estimates were completed by 9 localities. Though a small sampling, analysis shows:

- Size of locality does not necessarily imply greater elections security maturity
- Elections security maturity, even to these minimum standards, varies greatly.

Department of Elections (ELECT) staff recommendation:

ELECT staff recommends adoption of the proposed minimum security standards for immediate enactment.

INCIDENT REPONSE MINIMUM SECURITY STANDARD

PURPOSE

The purpose of this document is to establish minimum security standards for localities to mitigate security incident impact through development and dissemination of an incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Accordingly, ensure that locality incident response procedures implement required incident response policy and controls.

SCOPE

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

ROLES & RESPONSIBILITIES

- The Department of Elections standing advisory group (per HB2178; pursuant to subsection A of § 24.2-410.2 of the Code of Virginia) is responsible for the review, update and revision of this security standard and related standards on an annual basis or more frequently if needed.
- The locality Electoral Board is accountable and the locality Information Security Officer (ISO) or responsible party is responsible for adherence to this standard and documenting non-compliance via Department of Elections' exception handling.
- The locality ISO or responsible party is responsible for review, update and revision of this standard's procedures on an annual basis or more frequently if needed

INCIDENT RESPONSE TRAINING

1. The locality provides incident response training annually to information system users consistent with assigned roles and responsibilities. This training may be part of annual Computer Security Awareness training.
2. Simulated events or real world responses are incorporated into incident response training to facilitate effective response by personnel.

INCIDENT RESPONSE TESTING

1. The locality tests incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies; using checklists, walk-throughs and/or tabletop exercises, etc. This may or may not be accomplished as

part of other locality testing, such as Business Continuity, Disaster Recovery, Continuity of Operations, etc.

INCIDENT HANDLING AND RESPONSE

1. The locality:
   a. Recommendation: Implements an incident handling capability for security (and Privacy) incidents that includes preparation, detection and analysis, containment, eradication and recovery.
   b. Coordinates incident handling activities with contingency planning activities.
   c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, testing and implement resulting changes accordingly.
   d. Recommendation: Automated mechanisms are used to support the incident handling process, such as an online incident management system.
   e. Recommendation: Incident information and individual incident responses are correlated to achieve a locality wide perspective on incident awareness and response.
   f. Identifies immediate mitigation procedures, including specific instructions, based on information security incident type, on whether or not to shut down or disconnect affected IT systems.
   g. Establishes procedures for information security incident investigation, preservation of evidence, and forensic analysis.
2. The locality ISO or designee requires that system security incidents are tracked and documented including, but not limited to, the following information:
   a. Maintaining records about each incident.
   b. The status of the incident.
   c. Information necessary for forensics if applicable.
   d. Evaluating incident details, trends, and handling.
   e. Recommendation: Localities employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

INCIDENT REPORTING

1. The locality ensures reporting of Elections specific suspected and actual security incidents in accordance with the criteria and procedures set forth in the Department of Election's Incident Reporting guideline. Incidents should be reported to the Virginia Fusion Center email VFC@vsp.virginia.gov or call VFC at 804-674-2196. After calling the VCF, call the Department of Elections IT at 804-608-5653.

INCIDENT RESPONSE ASSISTANCE

1. The locality identifies an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents; recommend

employing automated mechanisms to increase the availability of incident response-related information and support. (i. e. a website, automatic email notifications, etc.)

INCIDENT RESPONSE PLAN

1. The locality has developed an incident response plan that:
    a. Provides the locality with a roadmap for implementing its incident response capability.
    b. Meets the unique requirements of the organization, which relate to mission, size, structure and functions.
    c. Defines reportable incidents.
    d. Is reviewed and approved by the locality ISO or designee.
2. Copies of the incident response plan are distributed as appropriate.
3. The incident response plan is reviewed at least annually and when there is an incident, based on lessons learned.
4. The incident response plan is updated to address changes or problems encountered during plan implementation, execution or testing.
5. The incident response plan is protected from unauthorized disclosure and modification.

PASSWORD MANAGEMENT MINIMUM SECURITY STANDARD

PURPOSE

The purpose of this document is to establish minimum security requirements for localities to mitigate the risk of unauthorized user access.

SCOPE

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

ROLES & RESPONSIBILITIES

- The Department of Elections standing advisory group (per HB2178; pursuant to subsection A of § 24.2-410.2 of the Code of Virginia) is responsible for the review, update and revision of this security standard and related standards on an annual basis or more frequently if needed.
- The locality Electoral Board is accountable, and the locality Information Security Officer (ISO) or responsible party is responsible, for adherence to this standard and documenting non-compliance via Department of Elections' exception handling.
- Users are accountable for keeping their passwords confidential.
- The locality ISO or responsible party is responsible for review, update and revision of this standard's procedures on an annual basis or more frequently if needed.

PASSWORD COMPOSITION

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

7. Recommendation: The Login Screen does not give any information about password characteristic requirements.

PASSWORD MANAGEMENT

1. Passwords are encrypted. [Recommendation: AES 256 (or higher/more secure) standard.]
2. Passwords are not shared.
3. Passwords are not displayed on screen on entry.
4. Users authenticate with current password before changing to a new one.
5. Recommendation: Access to the password storage location is highly limited.
6. Recommendation: Passwords are changed every 90 days. [Changed every 30 days if only 2 of the password character types are required; meaning, when weaker passwords are utilized.]
7. Recommendation: Any unsuccessful login attempt does not give the user any indication of what the password lacked. For example, if a user tries to log in unsuccessfully, they only receive a "Login Unsuccessful" message. No details of why the login was unsuccessful are provided to the user.
8. Recommendation: Password characteristics (length, complexity, etc.) are reviewed at least annually to ensure sufficient strength consistent with emerging technologies.

SECURITY ASSESSMENT AND AUTHORIZATION MINIMUM SECURITY STANDARD

PURPOSE

The purpose of this document is to establish minimum security standards for localities to conduct security assessments and turn the results into a risk-based report suitable for authorizing officials to approve the risk levels noted in the report.

SCOPE

This assessment and authorization standard applies to all information systems identified as sensitive to election related activities and their 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.

REQUIREMENTS

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

SECURITY ASSESSMENTS

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

4. Assessment results are provided as input into overall enterprise risk and compliance management processes. Recommendation: and should be an input to the locality's Capital Improvement/Spending plan.
5. Security and risk assessment processes are enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.
6. The locality mandates the development and periodic maintenance of system-specific security assessment plan(s) which describes:
   a. System(s) under assessment.
   b. Security controls and control enhancements under assessment.
   c. Assessment procedures to be used to determine security control effectiveness.
   d. Assessment environment, assessment team, and assessment roles and responsibilities.
7. A security assessment report is produced and documents the results of the assessment.
8. The results of the security control assessment are provided to senior security and business risk management leadership, including prioritized mitigations.

SYSTEM INTERCONNECTIONS

1. Authorizes connections from the information system to other information systems outside the Enterprise Security boundary or boundary for the server under assessment through the use of Interconnection Security Agreements (ISAs) (e.g. Electronic Pollbook). Note: Connections to General Support Systems and Office productivity are excluded. Also, connections within the enterprise to other servers (DB, Print, etc.) don't need ISAs. The security posture relative to the server in the assessment should be part of those components' assessment, which can be referenced.
2. Documents for each interconnection detail the interface characteristics and security requirements, and uses and sensitivity of the information communicated.
3. Recommendation: The ISAs detail how the data will be protected during transport, storage, and use. Particular attention is paid to the handling of Privacy or sensitive election related data.
4. Reviews and updates ISAs at least annually or when a major system change is planned to occur, prior to implementation.

FLAW REMEDIATION/PLAN OF ACTION AND MILESTONES

1. Develops a POA&M for the information system to
   document the locality's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. POA&Ms are prioritized, assigned personal ownership, and have target completion dates.

2. Existing POA&Ms are updated based on the findings from security controls assessments, security impact analyses and continuous monitoring activities. Recommendation: Any "high-dollar" mitigations are added to the locality's Capital Improvement/Spending plan.
3. The System Owner with assistance from the ISO or designee identifies, reports, and corrects or mitigates information system flaws (e.g. removing software or disabling functions, installing patches, making changes to configuration settings).
4. Inventory of information systems and components are collected and maintained in order to determine which hardware equipment, operating systems, and software applications are in operation (Hardware Asset Management – HWAM and Software Asset Management SWAM). Recommendation: The inventory is continually compared to the lists of authorized HW and SW or the Configuration Management Database (CMDB).
5. Inventory of information systems is updated to reflect current software configurations after remediation activities.
6. Prior to installation, software updates related to flaw remediation are tested for effectiveness and potential side effects on organizational information systems; testing includes checking all related software to ensure it is operating correctly.
7. Flaw remediation is incorporated into locality's configuration management process.
8. A Patch and Vulnerability Management Plan exists and addresses the following:
   a. All equipment, operating systems, and software applications are included. Note: If locality has hundreds of approved programs on network (i.e. mainly through grandfathering), suggest having authorizing official sign off with being OK with that situation or develop POA&Ms around those risks (if they intend to mitigate them).
   b. The responsible party for monitoring and coordinating with each vendor for patch release support is designated.
   c. Recommendation: Procedures for testing before putting into Enterprise-wide use.
9. Vulnerability and flaw remediation actions are tracked and verified.

SECURITY AUTHORIZATION

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

Recommendation: CONTINUOUS MONITORING

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

SECURITY AWARENESS TRAINING MINIMUM SECURITY STANDARD

PURPOSE

The purpose of this document is to establish minimum security standards for localities to develop compliant and effective Security Awareness training programs to lower the risk posed by locality system user personnel.

SCOPE

This security awareness training standard applies to all personnel having access to or responsibility for any information systems identified as sensitive to election related activities or their peripherals.

ROLES & RESPONSIBILITIES

- The Department of Elections standing advisory group (per HB2178; pursuant to subsection A of § 24.2-410.2 of the Code of Virginia) is responsible for the review, update and revision of this security standard and related standards on an annual basis or more frequently if needed.
- The locality Electoral Board is accountable and the locality Information Security Officer (ISO) or responsible party is responsible for adherence to this standard and documenting non-compliance via Department of Elections' exception handling.
- The locality ISO or responsible party is responsible for review, update and revision of this standard's procedures on an annual basis or more frequently if needed.

SECURITY AWARENESS TRAINING

The ISO or designee oversees Locality's Security Awareness and Training program, including but not limited to:

Development, implementation, and testing.
Coordinating, monitoring and tracking the completion of the Security Awareness Training for all employees, and reports incomplete training to the respective managers.

1. Developing an information security training program so that each IT system user is aware of and understands the following concepts and potential penalties for violations:
    a. The locality's policy for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data including Election information.
    b. The concept of separation of duties, least privilege, and elevated privileges.
    c. Prevention and detection of information security incidents, including those caused by malicious code Recommendation: and reporting to the Virginia Fusion Center at email VFC@vsp.virginia.gov or 804-674-2196, or in alignment with locality reporting procedures.
    d. Proper use of encryption and disposal of data storage media.
    e. Access controls, including creating and changing passwords and the need to keep them confidential.

f. Locality's acceptable use and Remote Access policies.
g. Intellectual property rights, including software licensing and copyright issues.
h. Special responsibility for the security of locality/ELECT and Privacy data.
i. Social engineering and phishing and other timely IT Security topics.

2. A variety of methods are used to deliver Security Awareness and Training to locality employees and business partners periodically throughout the year, and at least annually for full refresher training. Methods of delivery include, but are not limited to, in-person, online, one-on-one instruction, videos, blogs, social media, posters, newsletters, contests and events consistent with best practices.

ROLE BASE SECURITY TRAINING

The ISO or designee identifies opportunities to create the appropriate role-based information security training materials and communicates the training opportunities to managers. This training should happen;

- Before authorizing access to the information system or performing assigned duties
- When required by information system changes
- As practical and necessary thereafter.

Managers ensure that locality employees and business partners, who manage, administer, operate, or design IT systems, receive additional role-based information security training that is commensurate with their level of expertise.

SECURITY TRAINING RECORDS

The ISO or designee:

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

SYSTEM AND INFORMATION INTEGRITY MINIMUM SECURITY STANDARD

PURPOSE

The purpose of this document is to establish minimum security standards for localities to develop procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls. Accordingly, ensure that the system and information integrity procedures implement the requisite control sets per locality procedure.

SCOPE

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

ROLES & RESPONSIBILITIES

- The Department of Elections standing advisory group (per HB2178; pursuant to subsection A of § 24.2-410.2 of the Code of Virginia) is responsible for the review, update and revision of this security standard and related standards on an annual basis or more frequently if needed.
- The locality Electoral Board is accountable and the locality Information Security Officer (ISO) or responsible party is responsible for adherence to this standard and documenting non-compliance via Department of Elections' exception handling.
- The locality ISO or responsible party is responsible for review, update and revision of this standard's procedures on an annual basis or more frequently if needed.

MALICIOUS CODE PROTECTION

The locality ISO or designee utilizes real time malware/anti-virus/malicious code scanning and provides for full system scans on a regularly scheduled basis to be determined by the locality.

1. The locality ISO or designee requires that its service provider:
2. Ensures users and developers do not knowingly develop or experiment with malicious programs (e.g., viruses, worms, spyware, keystroke loggers, phishing software, Trojan horses, etc.).
3. Prohibits systems from being used in production until they have been properly configured/tested and have anti-malware protections installed and updated.
4. Anti-malware and spam controls are configured on email system(s) to limit unsolicited messages and updated when new releases are available and tested.

SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

1. The locality ISO or designee ensures:
    a. Internal security alerts, advisories, and directives are generated, as appropriate.
    b. Security alerts, advisories, and directives are disseminated to appropriate locality personnel.
    c. Recommendation: User or system compliance with security alerts, advisories, and directives, and determines risk posed by exceptions to the alert(s).

INFORMATION SYSTEM MONITORING

1. The locality ISO or designee enforces the following requirements:
    a. Information systems are monitored in accordance with laws, regulations, policies, defined monitoring objectives and implement measures to detect information system Unauthorized (local, network, and remote)use.
    b. Recommendation: Intrusion-monitoring tools and mechanisms are tested on a periodic basis defined by locality policy.
    c. Recommendation: A wireless intrusion detection capability is deployed to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.
    d. Recommendation: Network services/applications that have not been authorized by locality policy are detected.

SYSTEM AND COMMUNICATION PROTECTION MINIMUM SECURITY STANDARD

PURPOSE

The purpose of this document is to establish minimum security standards for localities to develop procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls.

SCOPE

This system and communication protection standard applies to all information systems identified as sensitive to election related activities and their 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.

BOUNDARY PROTECTION

1. The information system is configured to monitor and control communications at the external boundary of the system and key internal boundaries within the system.
2. Connections to external networks or information systems are via managed interfaces consisting of boundary protection devices (e.g., proxies, gateways, routers, firewalls, encrypted tunnels) arranged in accordance with an effective, security architecture.
3. Subnetworks are implemented for publicly accessible system components to separate them from internal organizational networks.
4. Boundary/edge devices (e.g., firewalls, routers) are configured to protect and control access to information resources.
5. Incoming network traffic is inspected and requests that do not comply with applicable policy are denied.
6. Logging features on firewalls and proxies log the occurrence of dropped packets, and locality staff or the entity managing the firewall reviews those logs in accordance with IT Operations procedures. For large systems, the use of log reduction and correlation software is recommended.
7. Firewall and router configurations and associated documentation are treated as confidentially sensitive information and are available to only authorized personnel (e.g., authorized administrators, auditors, security oversight personnel).
8. A secure method that supports encryption is used to access a router interface in order to prevent packet sniffing.

9. When securing networked hosts, unused or unneeded services and applications are disabled or if practical, removed.
10. Port protection capabilities (MAC Protection, Port Security, 802.1x, disabling unused ports, etc.) are utilized to prevent the connection of unauthorized equipment to the network.
11. Cryptographic mechanisms are implemented to prevent unauthorized disclosure or corruption of information and to detect changes to information during transmission. Highly sensitive files (e.g. Voter Registration) may need to use additional controls such as Hashing.
12. The locality ISO or designee, in conjunction with IT Operations:
    a. Assesses the risk of denial of service attacks to critical information systems and ensures that those risks are adequately addressed.
    b. Manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks.
    c. Employs monitoring tools to detect indications of denial of service attacks against the information systems, or works with service provider for alerts of abnormal traffic levels.

USE OF CRYPTOGRAPHY

1. The Locality ISO or designee ensures:
    a. Practices for selecting and deploying encryption technologies and for the encryption of data are defined and documented.
    b. All end-user systems (desktop, laptop, tablet, etc.) that are used to conduct locality business uses encryption to protect all information on their storage device.
    c. Transmission of sensitive data is encrypted.
    d. Digital signatures may be utilized for data integrity.

PERIPHERAL DEVICE ACCESS

1. The Locality ISO or designee ensures:
    a. Localities establish acceptable use policy for peripheral devices.
    b. Unneeded connection ports or input/output devices on information systems or information system components are disabled or removed.

ACCESS CONTROL MINIMUM SECURITY STANDARD

PURPOSE

The purpose of this document is to establish minimum security standards for localities to prevent unauthorized user access; verifying and validating users, and that they are permitted to use the systems and data they are attempting to access.

SCOPE

This access control standard applies to all information systems identified as sensitive to election related activities and their 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 also applies to all network-based and locally-based authentication and stand-alone systems utilized to gain access to these sensitive election related systems.

ROLES & RESPONSIBILITIES

- The Department of Elections standing advisory group (per HB2178; pursuant to subsection A of § 24.2-410.2 of the Code of Virginia) is responsible for the review, update and revision of this security standard and related standards on an annual basis or more frequently if needed.
- The locality Electoral Board is accountable, and the locality Information Security Officer (ISO) or responsible party is responsible, for adherence to this standard and documenting non-compliance via Department of Elections' exception handling.
- The locality ISO or responsible party approves and authorizes access to administrative or privileged accounts.
- System Owners and Supervisors are accountable for defining access privileges for each role, for reviewing the access privileges on a periodic basis, for ensuring that each user has only enough access to conduct their job, and for prohibiting privileged access by users who have not gone through the appropriate vetting processes.
- Individuals are accountable for activities performed under their user account.
- The locality ISO or responsible party is responsible for review, update and revision of this standard's procedures on an annual basis or more frequently if needed.

CONTROL AND ACTIVELY MANAGE ACCESS

1. The number of people with access to the system are limited to those who need it to complete their jobs.
2. What each user is authorized to do is restricted to using the principle of "least privilege;" users are given the minimum level of access that they require to perform their jobs.
3. Elevated permissions are not used on a day to day basis; the General User/Office Productivity account is used. Similarly, Privileged Users (system, network, ISOs, database admins, etc.) do not use their General User/Office Productivity account to perform work on the system(s) in

their charge. Those Privileged Users log on and use a separate privileged account for those activities.

4. Those who no longer need access are removed, regardless of their privilege level. This is part of the standard transfer and off-boarding procedures for staff.

Recommendations:

5. The application for a new user account lists the Role(s) the user will need to perform their business functions. Applicants or their Supervisors must explicitly list the systems and groups the user needs, prior to account approval and creation.
6. The use of Privileged Accounts are time limited for each session to 2 hours. Privileged Users have a forced logoff after 15 minutes of inactivity.
7. Privileged Accounts usage are logged and tracked separately from the use of General User accounts. At least quarterly, the ISO and System Owners review the Privileged Users and their activities on the system(s) for which they are accountable.
8. Any temporary, test or default accounts are removed from systems when not in use, or are kept in compliance with the organization's policies.
9. Network sign-on accounts are disabled from concurrent use, as are service accounts.

SEPARATION OF DUTIES

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

USER ACCOUNT CREATION

1. Each user has a unique ID for account access traceability. [Recommend the same for service accounts.]
2. Accounts are reviewed periodically and disabled if not in use.
3. Use of shared accounts and passwords are properly documented and authorized, and account credentials are reissued when individuals are removed from the group. [Recommendation: Shared/system accounts are only created or used on an "exception" basis. These exceptions are documented and noted as part of the system's Risk Assessment. They are reviewed quarterly by the ISO and System Owner.]

REMOTE ACCESS

1. Remote access users are identified, authenticated and authorized.
2. Remote access employs two-factor authentication and session timeout after no longer than 30 minutes of inactivity. [Recommend timeout after 15 minutes of inactivity.]
3. Auditable records of remote access are maintained.

ACCESS POINTS WITH A WIRELESS NETWORK

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

WIRELESS NETWORK SEGREGATION

1. Wireless Access Point access control features are logically or physically separated.
2. Wireless Access Points are configured to generate security logs and monitored for security issues.
3. Wireless traffic uses encryption. [Recommend encryption that meets NIST SP 800-53 and Federal Information Processing Standards (FIPS), such as FIPS 140-2.]

MANAGEMENT REQUIREMENTS

1. As applicable, detects rogue access points connected to the implemented wired network (i.e. via features in the Wireless Access Points or through a periodic discovery process) and mitigation occurs.
2. <u>Recommendation</u>: Accounts/Passwords are suspended within 24 hours after a user no longer requires access (termination, reassignment, etc.). If the loss of access was involuntary, the Accounts/Passwords are suspended as soon as the termination occurs.
3. <u>Recommendation</u>: Confirmation of Access controls is validated at least annually. [Typically, the validation is confirmed by a combination of vulnerability and penetration testing.]
4. <u>Recommendation</u>: Localities use Role Based Access (RBAC) to the greatest extent possible. This means promoting the use of Group Accounts based on a user's business needs and eliminating/severely restricting use of individual network and local accounts on a system's Access Control List (ACL).

SESSION LOCK OUT

1. A session locking policy is implemented that prevents further access to the system by initiating a session lock out.
2. Accounts are locked after a maximum of no more than 30 minutes of inactivity, and reestablished access after user authenticates. [<u>Recommendation</u>: after 15 minutes of inactivity.]

MOBILE DEVICES

1. Mobile devices that contain elections specific data, are encrypted to protect the confidentiality and integrity of that information. [<u>Recommendation</u>: Encryption is AES 256 compliant and applies to data storage and transmission (where applicable).]

UNSUCCESSFUL LOGON ATTEMPTS

1. Enforces a limit of consecutive invalid logon attempts (to be determined by locality) by a user during a 15 minute period. [<u>Recommendation</u>: Accounts are locked after a maximum of five unsuccessful access attempts, and the account is only unlocked by the Help Desk or automated account service system.]
2. <u>Recommendation</u>: Users are not provided 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. No details of why the login was unsuccessful are provided to the user.

SYSTEM USE NOTIFICATION

1. Employs system use notification message or banner, which provides privacy and security notices, before granting access to the system.
2. Recommendation: The System Logon message or banner does not give any indication of the system name or password requirements for the system being logged into.

CONTINGENCY PLANNING MINIMUM SECURITY STANDARD

PURPOSE

The purpose of this document is to develop, document, and disseminate to a contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and facilitates the implementation of the contingency planning policy and the associated contingency planning controls.

SCOPE

Contingency Planning is conducted for all election related business processes and associated information systems identified as sensitive to election related activities, to include applications, servers, computers, and networks; that process, store, access or transmit voter registration system related information. This standard also applies to any locality employees (classified, hourly, and/or business partners) who also participate in election related activities.

ROLES & RESPONSIBILITIES

- The Department of Elections standing advisory group (per HB2178; pursuant to subsection A of § 24.2-410.2 of the Code of Virginia) is responsible for the review, update and revision of this security standard and related standards on an annual basis or more frequently if needed.
- The locality Electoral Board is accountable and the locality Information Security Officer (ISO) or responsible party is responsible for adherence to this standard and documenting non-compliance via Department of Elections' exception handling.
- The locality ISO or responsible party is responsible for review, update and revision of this standard's procedures on an annual basis or more frequently if needed.

DEFINITONS

1. Business Impact Assessment (BIA): This process develops a list of all core functions that an organization or locality performs in support of the successful completion of their business mission or goals. Specifically excluded from the BIA are supporting functions such as IT, HR, Financial Management, and other administrative areas. Once the list of core business functions is developed, the BIA will then determine the impact of the loss or degradation of the functions with respect to the mission goals. Finally the BIA will determine the priority of the functions in relation to the organizations mission and goals.
2. Continuity of Operations Plan (COOP): This plan uses the BIA as an input and then develops a prioritized list of tasks, activities, resources, and supporting functions that are necessary ensure that the core business can be carried out in a manner meeting the functional requirements of those business area.

3. Contingency Plan (CP): The CP takes the COOP and BIA to develop a list of what people, tools, technologies, processes, and support functions must be in place to resume normal or possibly degraded functionality when one or more threats materialize to place the mission of the organization in jeopardy. Some examples of threats include, but are not limited to:

    - Damaging weather (wind/flood, etc.)
    - Civil Unrest
    - Cyber Attack
    - Loss of Power or Internet Service
    - Insider Malfeasance

    There are other plans and documents that the CP will also draw on to come up with a complete picture of threats and how to mitigate at the locality level. Some of these include a Personnel Evacuation Plan, an Alternate Processing Facility Plan, an Employee Remote Work plan, the Enterprise Architecture plan and others as needed.

CONTINGENCY PLAN

1. A contingency plan is developed that:
    a. Identifies essential missions and business functions and associated contingency requirements.
    b. Provides recovery objectives, restoration priorities, and metrics.
    c. Addresses contingency roles, responsibilities, assigned individuals with contact information.
    d. Addresses maintaining essential missions and business functions despite a system disruption, compromise, or failure.
    e. Addresses eventual, full system restoration without deterioration of the security and privacy controls originally planned and implemented.
    f. Is reviewed and approved by the locality GR and Electioral Board.
2. Contingency plan development is coordinated with the organizational elements responsible for related plans. Examples are Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.
3. Critical system assets supporting essential missions and business functions are identified.
4. The contingency plan is coordinated with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.
5. The plan accounts for the transfer of essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.
6. The plan accounts for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.

7. Capacity planning is conducted so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

CONTINGENCY TRAINING

1. Contingency training is provided to system users consistent with assigned roles and responsibilities in the CP process.
2. Simulated events are incorporated into contingency training to facilitate effective response by personnel in crisis situations.

CONTINGENCY PLAN TESTING

1. The contingency plan for the system is periodically tested using varying methods (Table top, partial shutdown, penetration tests, etc.) to determine the effectiveness of the plan and the organizational readiness to execute the plan review the test results and initiate corrective actions, if needed. Recommendation: Testing of plan alternates annually between Table top and full recovery. (i.e. Table top in 2020, Full recovery in 2021, etc.)
2. Contingency plan testing is coordinated with other locality elements responsible for related plans.
3. The contingency plan is tested at the alternate processing site to familiarize contingency personnel with the facility and available resources and evaluate the capabilities of the alternate processing site to support contingency operations.
4. Full recovery and reconstitution of the system to a known state is included as part of contingency plan testing.

ALTERNATE PROCESSING and STORAGE SITES

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

TELECOMMUNICATIONS SERVICES

1. Primary and alternate telecommunications service agreements are developed that contain priority-of-service provisions in accordance with locality availability requirements.
2. Alternate telecommunications services are obtained from providers that are separated from primary service providers to reduce susceptibility to the same threats.
3. Primary and alternate telecommunications service providers are required to have contingency plans that meet locality contingency requirements and obtain evidence of contingency testing and training by providers.

4. Alternate telecommunication services are tested on a regular basis consistent with locality IT requirements.

SYSTEM BACKUP

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

SYSTEM RECOVERY AND RECONSTITUTION

1. Provide the capability to restore system components within the COOP, from configuration-controlled and integrity-protected information representing a known, operational state for the components.
2. Protect system components used for backup and restoration. Protection of system backup and restoration components (hardware, firmware, and software) includes both physical and technical safeguards.

ALTERNATIVE SECURITY MECHANISMS

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

MAINTENANCE MINIMUM SECURITY STANDARD

PURPOSE

The purpose of this document is to establish minimum security standards for localities to develop procedures facilitating the implementation of the system maintenance policy and the associated system maintenance controls.

SCOPE

This standard addresses the 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; i.e. in-contract, warranty, in-house, software maintenance agreement, etc.). System maintenance also includes those components not directly associated with information processing and/or data information retention such as scanners, copiers and printers.

ROLES & RESPONSIBILITIES

- The Department of Elections standing advisory group (per HB2178; pursuant to subsection A of § 24.2-410.2 of the Code of Virginia) is responsible for the review, update and revision of this security standard and related standards on an annual basis or more frequently if needed.
- The locality Electoral Board is accountable and the locality Information Security Officer (ISO) or responsible party is responsible for adherence to this standard and documenting non-compliance via Department of Elections' exception handling.
- The locality ISO or responsible party is responsible for review, update and revision of this standard's procedures on an annual basis or more frequently if needed.

CONTROLLED MAINTENANCE

The locality approves and monitors all maintenance activities, whether performed within the locality (on site or locality-controlled) or remotely, and whether the equipment is serviced on site or removed to another location; *including consideration of supply chain issues associated with replacement components for information systems as appropriate.*

1. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.
2. Requires that locality-defined personnel/roles explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.
3. Sanitizes equipment to remove all information from associated media prior to removal from locality facilities for off-site maintenance or repairs.
4. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

5. Includes locality-defined maintenance-related information in the maintenance records, as appropriate, in addition to items such as:
   a. Date and time of maintenance.
   b. Name of individuals or group performing the maintenance.
   c. Name of escort, if necessary.
   d. Description of the maintenance performed.
   e. Information system components/equipment removed or replaced (including identification numbers if applicable).
6. The level of detail included in maintenance records is appropriate to the security categories of locality information systems.

MAINTENANCE TOOLS

This addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on locality information systems. Maintenance tools can include hardware, software and firmware items, and are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into locality information systems.

The locality:

1. Inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.
2. Checks media containing diagnostic and test programs for malicious code before the media are used in the information system. E.g. setting anti-virus to force a scan on any removable media.
3. Prevents the unauthorized removal of maintenance equipment containing locality information by one of the following:
   a. Verifying that there is no locality information (specific to the locality or for which the locality serves as information stewards) contained on the equipment.
   b. Sanitizing or destroying the equipment.
   c. Retaining the equipment within the facility.
   d. Obtaining an exemption from locality authorized personnel explicitly authorizing removal of the equipment from the facility.
4. Restricts the use of maintenance tools to authorized personnel only. E.g. This could be done by establishment of a policy stating “Use of maintenance tools are restricted to authorized personnel only.”

NON-LOCAL MAINTENANCE

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

The locality:

1. Approves and monitors non-local maintenance and diagnostic activities.
2. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system.
3. Employs strong authenticators in the establishment of non-local maintenance and diagnostic sessions.
4. Maintains records for nonlocal maintenance and diagnostic activities.
5. Terminates session and network connections when non-local maintenance is completed.

MAINTENANCE PERSONNEL

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

1. The locality ensures that anyone who has access has been properly vetted and is escorted where required.

TIMELY MAINTENANCE

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

MEDIA PROTECTION MINIMUM SECURITY STANDARD

PURPOSE

The purpose of this document is to establish minimum security standards for localities to develop procedures to implement as risk control measures associated with the various forms of media in use.

SCOPE

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

ROLES & RESPONSIBILITIES

- The Department of Elections standing advisory group (per HB2178; pursuant to subsection A of § 24.2-410.2 of the Code of Virginia) is responsible for the review, update and revision of this security standard and related standards on an annual basis or more frequently if needed.
- The locality Electoral Board is accountable and the locality Information Security Officer (ISO) or responsible party is responsible for adherence to this standard and documenting non-compliance via Department of Elections' exception handling.
- The locality ISO or responsible party is responsible for review, update and revision of this standard's procedures on an annual basis or more frequently if needed.

MEDIA ACCESS

1. The ISO or designee requires that access to digital and non-digital media is restricted to authorized individuals only.
2. Assessment of risk guides the selection of media, and associated information contained on that media requiring restricted access.
3. System Owners document policies and procedures for the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access.

MEDIA STORAGE

1. The ISO or designee implements and documents procedures to safeguard handling of all backup media containing sensitive data. At a minimum, these procedures include the following requirements:

a. Employing cryptographic mechanisms to protect information in storage where the data is sensitive as related to confidentiality.
b. Physically control and secure storing digital and non-digital media within locality-defined controlled areas using defined security measures until the media is destroyed or sanitized using approved equipment's, techniques, and procedures.

ELECTIONS SENSITIVE DATA MEDIA TRANSPORT

The ISO or designee requires:

1. All digital and non-digital media is protected and controlled during transport outside of controlled areas using organization-defined security measures (i.e., locked container, cryptography).
2. Accountability for information system media is maintained during transport outside of controlled areas, custodians must immediately report loss or theft of any assets.
3. Activities associated with the transport of information system media must be documented. Employees must not remove locality or business partner owned IT assets from premises unless for a documented approved reason.
4. The ISO or designee documents, using established documentation requirements, activities associated with the transport of information system media in accordance with risk assessment. At a minimum, any log or tracking mechanism includes:
   a. Description of information being transported.
   b. Type of Information (e.g. PII) contained on the media
   c. Method(s) of transport.
   d. Protection methods employed.
   e. Name(s) of individual(s) transporting the information.
   f. Authorized recipient(s) where practical/applicable.
   g. Dates sent and received.

MEDIA DESTRUCTION/SANITIZATION

1. The ISO or designee requires that information system media, both digital and non-digital, is sanitized prior to disposal, release out of organizational control, or release for reuse.
2. Media sanitization and disposal actions are tracked, documented, and is verifiable.
3. One of the following three acceptable methods are used for the removal of digital data from any media commensurate with the security category or classification of the information:
   a. DOD/NIST approved Overwriting – Overwriting is an approved method for removal of Commonwealth data from hard disk storage media. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information.
   b. Degaussing – A process whereby the magnetic media are erased, (i.e., returned to a zero state). Degaussing (demagnetizing) reduces the magnetic flux to virtual

zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable by keyboard or laboratory attack.

c. Physical Destruction – Hard drives are physically destroyed when they are defective or cannot be economically repaired or Commonwealth data cannot be removed for reuse. Physical destruction is accomplished to an extent that precludes any possible further use of the hard drive

PERSONNEL SECURITY MANAGEMENT MINIMUM SECURITY STANDARD

PURPOSE

The purpose of this document is for localities to develop and implement policies and procedures to ensure that employees and business partners comply with the minimum security prerequisites applicable to their function at the locality, and are informed of their responsibility to protect locality information.

Recommendation: Localities require that individuals undergo a specific screening process if their duties or tasks involve access to sensitive information and assets. Until the required controls are completed, individuals cannot be appointed to a position or have access to sensitive information and assets.

SCOPE

This standard applies to any locality employees (classified, hourly) and business partners who participate in election related activities. This also includes, but is not limited to, personnel with access (both general and privileged users) to information systems identified as sensitive to election related activities; to include applications, servers, computers, devices and networks that process, store, access or transmit voter registration system related information.

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

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

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

ROLES & RESPONSIBILITIES

- The Department of Elections standing advisory group (per HB2178; pursuant to subsection A of § 24.2-410.2 of the Code of Virginia) is responsible for the review, update and revision of this security standard and related standards on an annual basis or more frequently if needed.
- The locality Electoral Board is accountable and the locality Information Security Officer (ISO) or responsible party is responsible for adherence to this standard and documenting non-compliance via Department of Elections' exception handling.
- Those in charge of recruiting are responsible for ensuring that the selected applicant meets the security requirements needed on the basis of the level of access to information and assets that the job duties requires.

- Managers are responsible for performing screening during the course of the employment/contract according to the degree of sensitivity of the IT assets the individual may have access to.
- Managers are responsible for communicating to the staff their security responsibilities.
- Managers are responsible to communicate to employees and third party its security responsibilities and ensure familiarization with locality Information Security Policy and locality Security and Acceptable Use Policy.
- Locality General Registrar or responsible party is responsible for notifying ELECT of personnel transfers or terminations if the individual has a VERIS account.
- The locality ISO or designee periodically reviews and confirms ongoing operational need for current logical and physical access.
- The locality ISO or responsible party is responsible for review, update and revision of this standard's procedures on an annual basis or more frequently if needed.

PERSONNEL SCREENING

1. Localities will conduct background checks (education, work experience, criminal, credit check, etc.) prior to authorizing access to the information system.

PERSONNEL TERMINATION

1. If the user has a VERIS account, the general registrar or responsible party will notify ELECT (during working hours) within 4 hours of termination if voluntary and within 1 hour if involuntary. Notifications are made via email to electit@elections.virginia.gov.
2. Locality security manager or responsible party, in conjunction with IT, terminates/ revokes any authenticators/credentials associated with the individual.
3. Designated locality officials retrieve the appropriate assets (laptops, ID's, remote access tokens, removable media, etc.).

PERSONNEL TRANSFER

1. <u>Recommendation</u>: There exists an On-Boarding/Transfer/Off-Boarding process and work flow for required approvals and notifications to bring on new people, transfer existing personnel, and terminate existing personnel.
2. Locality IT or responsible party modifies access authorization as needed.
3. Locality IT or responsible party initiates the transfer or reassignment actions within 4 hours of the formal transfer action.
4. The locality ISO or designee periodically reviews and confirms ongoing operational need for current logical and physical access.

PERSONNEL ACCESS AGREEMENT

1. Access agreements have been developed and documented including Non-Disclosure Agreements (NDAs) for Sensitive systems.
2. Individuals requiring access to organizational information and information systems have signed appropriate access agreements. [Recommendation: Responsible locality entity ensures the appropriate access agreement/s has/have been signed and are retained in a secure location, in accordance with locality record retention policies. The base agreements are reviewed annually and changed if needed.]

VENDOR OR THIRD PARTY PERSONNEL ACCESS – contractor/consultant badge issued

1. As part of contracts or SLAs, Third Party entity is required to perform the appropriate background checks of their personnel, and to notify the localities when the entity's personnel are transferred or terminated.

PERSONNEL SANCTION

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

PHYSICAL ACCESS AND SECURITY MINIMUM SECURITY STANDARD

PURPOSE

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

SCOPE

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

ROLES & RESPONSIBILITIES

- The Department of Elections standing advisory group (per HB2178; pursuant to subsection A of § 24.2-410.2 of the Code of Virginia) is responsible for the review, update and revision of this security standard and related standards on an annual basis or more frequently if needed.
- The locality Electoral Board is accountable and the locality Information Security Officer (ISO) or responsible party is responsible for adherence to this standard and documenting non-compliance via Department of Elections' exception handling.
- The locality ISO or responsible party approves and authorizes access to restricted access area(s).
- Managers are accountable for defining physical access privileges for each role, for reviewing the physical access privileges on a periodic basis, for ensuring that each individual has only enough physical access to conduct their job, and for prohibiting unescorted physical access to restricted areas by non-locality individuals.
- Individuals are accountable for keeping any issued keys, badges, ID's, smart cards, etc. secure and not allowing others to borrow them.
- The locality ISO or responsible party is responsible for reviewing the physical access list and logs quarterly or as appropriate.
- The locality ISO or responsible party is responsible for review, update and revision of this standard's procedures on an annual basis or more frequently if needed.

PHYSICAL ACCESS AUTHORIZATIONS (RESTRICTED ACCESS AREA)

1. Access is restricted to authorized personnel through keys, combinations, badges, ID's, smart cards, etc. and individuals are given the minimum level of access that they require to perform their jobs.
2. Access list is reviewed quarterly or as appropriate.

3. Physical access is disabled for those who no longer need access, including terminated employees; immediately disabled for those who are terminated by management decision, otherwise when no longer needed.
4. As appropriate, access control is implemented to prevent shoulder surfing for output devices (e.g. monitors, printer room).
5. Keys, combinations, badges, and other physical access devices are secured.

MONITOR PHYSICAL ACCESS

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

ACCESS RECORDS FOR SECURE AREAS

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

PHYSICAL AND ENVIRONMENTAL PROTECTION MINIMUM SECURITY STANDARD

PURPOSE

The purpose of this document is to establish minimum security standards for localities to develop procedures to facilitate the implementation of physical and environmental security policy and the associated system and information integrity controls. Accordingly, ensure that the physical and environmental protection procedures are implemented per the requisite locality control sets and measure performance against those controls.

SCOPE

Recommendation: This physical and environmental protection standard applies to all locality controlled facilities and those facilities or premises controlled by locality vendors or Third Party Associate organizations. **NOTE: None of this standard is required; recommended only.**

ROLES & RESPONSIBILITIES

- The Department of Elections standing advisory group (per HB2178; pursuant to subsection A of § 24.2-410.2 of the Code of Virginia) is responsible for the review, update and revision of this security standard and related standards on an annual basis or more frequently if needed.
- The locality Electoral Board is accountable and the locality Information Security Officer (ISO) or responsible party is responsible for adherence to this standard and documenting non-compliance via Department of Elections' exception handling.
- The locality ISO or responsible party is responsible for review, update and revision of this standard's procedures on an annual basis or more frequently if needed.

Recommendation: POWER EQUIPMENT AND POWER CABLING

The ISO or designee requires that power equipment and power cabling for the information system is protected from damage and destruction.

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

Recommendation: EMERGENCY POWER

The ISO or designee:

1. Ensures a short-term uninterruptible power supply (UPS) or a generator is installed to facilitate an orderly shutdown of the information system in the event of a primary power source loss.
    a. The UPS and generators are tested by a certified technician at least once a year or when any material change is made to the UPS/generator. For facilities (remote, temporary, etc.) using small or individual machine UPS backup, the UPS is tested as part of periodic Contingency testing.
    b. Servers and critical hardware devices are protected by a UPS, installed either centrally or locally.

Recommendation: LOCATION OF INFORMATION SYSTEM COMPONENTS

The ISO or designee requires that:

1. Information system components are positioned within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. E.g. If water pipes are running overhead or automatic fire suppression sprinklers, then cabling or equipment is not placed underneath the pipes, or cover equipment nightly with waterproof coverings.
2. For existing facilities, the physical and environmental hazards are considered in the risk mitigation strategy for the information system.

Recommendation: TEMPERATURE AND HUMIDITY CONTROLS

1. The temperature and humidity levels are monitored and maintained where information system resides at organization-defined acceptable levels.

PROGRAM MANAGEMENT MINIMUM SECURITY STANDARD

PURPOSE

The purpose of this document is to establish the baseline security requirements that must be met to ensure that localities provide for the proper use and protection of its information assets; *especially related to the scope of Virginia's House Bill 2178 (HB2178)*.

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

An effective Information Security program:

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

SCOPE

This standard applies to the development, implementation and governance of the locality Information Security Program and Plan related to information systems classified as sensitive to election related activities, and should be aligned with the locality Information Security Program and Plan as appropriate.

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

ROLES & RESPONSIBILITIES

- The Department of Elections standing advisory group (per HB2178; pursuant to subsection A of § 24.2-410.2 of the Code of Virginia) is responsible for the review, update and revision of this security standard and related standards on an annual basis or more frequently if needed.
- The locality Electoral Board is accountable and the locality Information Security Officer (ISO) or responsible party is responsible for adherence to this standard and documenting non-compliance via Department of Elections' exception handling.
- The locality ISO or responsible party is responsible for review, update and revision of this standard's procedures on an annual basis or more frequently if needed.

ENTERPRISE GOVERNANCE AND INFORMATION SECURITY

1. The electoral board of each county and city that utilizes supporting technologies to maintain and record registrant information is the information security and privacy risk owner, *per HB 2178 § 24.2-410.2 Security of the Virginia voter registration system*.
2. Ensure Information Security governance is aligned with the locality enterprise governance, including capital planning and investment requests, and resources are available as planned; all exceptions are documented and reviewed by the electoral board.
3. The locality documents mission/business process definitions and associated information protection requirements in accordance with locality policy and procedure.
4. Information protection and privacy needs are derived from the mission/business needs defined by the locality, and are technology-independent.
5. Protection strategies are based on the prioritization of critical assets and resources. Note: Elections is part of the nation's critical infrastructure.

RISK MANAGEMENT

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

INFORMATION SECURITY PROGRAM & INFORMATION SECURITY PLAN

1. Develop, implement and maintain a locality Information Security Program and Plan.
2. The Information Security Plan should be reviewed periodically to ensure ongoing alignment, at least annually for incremental improvements. Recommendation: Plan is reviewed quarterly.

SECURITY PLANNING MINIMUM SECURITY STANDARD

PURPOSE

The purpose of this document is to establish minimum security standards for localities to facilitate the implementation of the security and privacy planning policies and the implementation of associated security and privacy planning controls.

SCOPE

This security planning standard applies to all organizations which support information systems identified as sensitive to election activities and their components. Components include, but are not limited to, user productivity systems (laptops/desktops as similarly configured groups), application servers, mobile devices (with similar configurations), network peripherals (printers, scanner, etc.), network infrastructure (routers, switches, firewalls, intrusion detection systems, file servers, databases, system monitoring and security tools, etc.), and Cloud assets.

ROLES & RESPONSIBILITIES

- The Department of Elections standing advisory group (per HB2178; pursuant to subsection A of § 24.2-410.2 of the Code of Virginia) is responsible for the review, update and revision of this security standard and related standards on an annual basis or more frequently if needed.
- The locality Electoral Board is accountable and the locality Information Security Officer (ISO) or responsible party is responsible for adherence to this standard and documenting non-compliance via Department of Elections' exception handling.
- The locality ISO or responsible party is responsible for review, update and revision of this standard's procedures on an annual basis or more frequently if needed.

SYSTEM SECURITY PLAN

The locality:

1. Develops a security plan for the information system that:
    a. Is consistent with the organization's enterprise architecture.
    b. Explicitly defines the authorization boundary for the system.
    c. Describes the operational context of the information system in terms of missions and business processes.
    d. Provides the security categorization of the information system and relationships with or connections to other information systems.
    e. Provides an overview of the security requirements for the system.
    f. Identifies any relevant overlays, if applicable.
    g. Describes the security controls in place or planned for meeting those requirements, including a rationale for the tailoring decisions.
    h. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

2. Distributes copies of the security plan and communicates subsequent changes to the plan as appropriate.
3. Reviews the security plan for the information system at least annually.
4. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.
5. Protects the security plan from unauthorized disclosure and modification.
6. Defines the security architecture.

SYSTEM AND SERVICES ACQUISITION MINIMUM SECURITY STANDARD

PURPOSE

The purpose of this document is to establish minimum security standards for localities to establish procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls to mitigate risk associated with those acquisitions.

SCOPE

This system and service acquisition standard applies to all information systems identified as sensitive to election activities, their individual components, and any services acquired to support those systems. Components include, but are not limited to, user productivity systems (laptops/desktops as similarly configured groups), application servers, mobile devices (with similar configurations), network peripherals (printers, scanner, etc.), network infrastructure (routers, switches, firewalls, intrusion detection systems, file servers, databases, system monitoring and security tools, etc.), and Cloud assets. Services can be any kind that supports the systems, including (but not limited to) technical administrators and subject matter experts, business and management analysts, administrative assistants, and others.

ROLES & RESPONSIBILITIES

- The Department of Elections standing advisory group (per HB2178; pursuant to subsection A of § 24.2-410.2 of the Code of Virginia) is responsible for the review, update and revision of this security standard and related standards on an annual basis or more frequently if needed.
- The locality Electoral Board is accountable and the locality Information Security Officer (ISO) or responsible party is responsible for adherence to this standard and documenting non-compliance via Department of Elections' exception handling.
- The locality ISO or responsible party is responsible for review, update and revision of this standard's procedures on an annual basis or more frequently if needed.

ACQUISITION GOVERNANCE

1. Resources required to protect the information assets are allocated as part of its planning and investment control process; *such as establishment of budget line item(s) for information security in locality programming and budgeting documentation*.

<u>Recommendation</u>: ACQUISITION PROCESS

1. Process includes incorporation of security-specific requirements commensurate with the type (hardware, software, services) and level of assurance of items being acquired; including but not limited to:
   a. Personnel providing services are appropriately trained related to integrating security within the system development life cycle.
   b. Security requirements and security-related documentation requirements.

   c. Requirements for protecting security-related documentation in accordance with the risk management strategy.
   d. Administrator documentation for the information system, component or service that describes:
      i. Secure configuration, installation and operation of the system, component or service.
      ii. Effective use and maintenance of security functions/mechanisms.
      iii. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.
      iv. Methods for user interaction, which enables individuals to use the system, component or service in a more secure manner.
      v. User responsibilities in maintaining the security of the system, component or service.
   e. Description of the information system development environment and environment in which the system is intended to operate.
      i. Acceptance criteria.
      ii. Personnel Security.
      iii. Requires compliance with locality information security requirements and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance.
      iv. Defines and documents government oversight and user roles and responsibilities with regard to information system services and monitoring on an ongoing basis.
2. Threats, vulnerabilities, and consequences are used to identify the security requirements of the hardware, software and/or services in terms of business requirements.

ACQUISITION MANAGEMENT

1. The procurement process is periodically assessed, improvement areas identified and enhancements implemented.
2. Information system components are replaced when components can no longer be appropriately supported or it is cost prohibitive.
3. Justification is provided with documented approval for the continued use of unsupported system components required to satisfy mission/business needs.

CONFIGURATION MANAGEMENT MINIMUM SECURITY STANDARD

PURPOSE

The purpose of this document is to establish minimum security requirements regarding configuration management, to help localities mitigate the risk of unauthorized changes being introduced into information systems without proper approval.

SCOPE

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

ROLES & RESPONSIBILITIES

- The Department of Elections standing advisory group (per HB2178; pursuant to subsection A of § 24.2-410.2 of the Code of Virginia) is responsible for the review, update and revision of this security standard and related standards on an annual basis or more frequently if needed.
- The locality Electoral Board is accountable and the locality Information Security Officer (ISO) or responsible party is responsible for adherence to this standard and documenting non-compliance via Department of Elections' exception handling.
- The locality ISO or responsible party is responsible to periodically review locality assets and baseline configurations. [Recommendation: Reviews to occur once a year at minimum, when an integral component is installed or upgraded, there is a significant configuration change, or demonstrated vulnerability.]
- The locality ISO or responsible party is responsible for review, update and revision of this standard's procedures on an annual basis or more frequently if needed.

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

1. A list of the approved hardware and software assets is maintained (preferably within a secure Configuration Management Database (CMDB) or spreadsheet).

2. Baseline configuration data is maintained, which documents the application of security configurations; including over time as changes are made.
3. A list of discovered hardware and software assets is periodically reviewed against known/approved lists.
4. Recommendation: Report differences in discovered versus approved configurations to the locality ISO and Help Desk, or in alignment with locality policy.

CHANGE CONTROL

1. Consideration for the security impact of configuration changes is a part of the approval process.
2. System and architectural changes are analyzed for security ramifications.
3. Configuration change decisions are documented and only approved changes are implemented.
4. Before and after change activities are audited against activities required to make changes, as appropriate.
5. Third parties are required to also implement configuration management and change control practices as part of contract Terms and Conditions or SLAs, where appropriate.

ACCESS RESTRICTION FOR CHANGE

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

INFORMATION SYSTEM COMPONENT INVENTORY

1. Approved system (HW/SW) component information is documented and maintained in a format usable/consumable by the localities' Asset Management system.
2. Recommendation: A process is developed and implemented to detect and investigate any device or software found on the network or components not listed as "Approved" in the Asset Management system.

CONFIGURATION MANAGEMENT PLAN

1. A Configuration Management plan is implemented that defines and assigns responsibility for developing, implementing, maintaining, testing, and decommissioning configuration items throughout the System Development Life Cycle.

2. Configuration Management approval includes stakeholders who are responsible for reviewing and approving proposed changes, including a security personnel that would conduct an impact analysis.

USER-INSTALLED SOFTWARE

1. Software authorization/approval policies are established, monitored, tested, and enforced.
2. Appropriate personnel are alerted when unauthorized software is detected, in alignment with locality policy.

AUDIT AND ACCOUNTABILITY MINIMUM SECURITY STANDARD

PURPOSE

The purpose of this document is to establish minimum security standards for localities to develop and deploy procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls. Additionally, this standard ensures that the audit and accountability procedures implement applicable audit and accountability policy and controls.

SCOPE

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

ROLES & RESPONSIBILITIES

- The Department of Elections standing advisory group (per HB2178; pursuant to subsection A of § 24.2-410.2 of the Code of Virginia) is responsible for the review, update and revision of this security standard and related standards on an annual basis or more frequently if needed.
- The locality Electoral Board is accountable and the locality Information Security Officer (ISO) or responsible party is responsible for adherence to this standard and documenting non-compliance via Department of Elections' exception handling.
- The locality ISO or responsible party is responsible for review, update and revision of this standard's procedures on an annual basis or more frequently if needed.

AUDITABLE EVENTS

1. Information Systems, at a minimum, must be capable of and configured to produce audit logs with the necessary event information.
2. End-user workstations, including but not limited to desktop and laptops, must also maintain logs of security related events.

CONTENT OF AUDIT RECORDS

1. The system is configured such that the audit records contain sufficient information to meet the unique requirements of the organization, which relate to mission, size, structure and functions at a minimum to:
   a. Establish what actions were taken, who took the actions, and on what date/time the actions were taken on the system.
   b. Provide forensic results and reporting capabilities.
2. Log additional information commensurate with the sensitivity of information system.

3. The system is configured to generate time stamps to include both date and time.
4. Whenever possible, all systems utilize Network Time Protocol (NTP) time synchronization.

AUDIT STORAGE CAPABILITY

1. Audit storage capacity is allocated such that capacity is not exceeded or information overwritten.
2. Recommendation: Automated alerts are provided when log storage capacity reaches pre-defined levels (50%, 80%, and 95%).
3. Information systems classified as sensitive are configured to off-load audit records at least once every 30 days onto a different system or media than the system being audited. Recommendation: Off-loaded data is stored offsite on a media or system that is not accessible to the same users (including privileged users) of the information system that produced the audit records." OR do you recommend not changing?

RESPONSE TO AUDIT PROCESSING FAILURES

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

AUDIT REVIEW, ANALYSIS, AND REPORTING

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

PROTECTION OF AUDIT INFORMATION

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

AUDIT RECORD RETENTION

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

POLICIES AND PROCEDURES MINIMUM SECURITY STANDARD

PURPOSE

This standard establishes the baseline security requirements that must be met to ensure that localities implement internal administrative, personnel, operational and technical policies and procedures to support information security program goals and objectives, and compliance. Where policies and procedures are not in alignment or missing, they will be updated or created.

SCOPE

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

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

ROLES & RESPONSIBILITIES

- The Department of Elections standing advisory group (per HB2178; pursuant to subsection A of § 24.2-410.2 of the Code of Virginia) is responsible for the review, update and revision of this security standard and related standards on an annual basis or more frequently if needed.
- The locality Electoral Board is accountable and the locality Information Security Officer (ISO) or responsible party is responsible for adherence to this standard and documenting non-compliance via Department of Elections' exception handling.
- The locality ISO or responsible party is responsible for review, update and revision of this standard's procedures on an annual basis or more frequently if needed.

LOCALITY RESPONSIBILITIES

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

ACCOUNTABILITY

1. Various locality leaders (Electoral Board, GR, CIO, ISO, IT Directors, etc.) are accountable to ensure compliance with this standard.
2. Compliance with this standard should be measured by both internal and external audits of the localities' IT Security policies and procedures against the Minimum Security Standards adopted by the VA State Board of Elections.

GENERAL IT SECURITY POLICY AND PROCEDURE

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

ADMINISTRATIVE POLICIES AND PROCEDURES

1. Security planning policy and procedures which provide for the effective planning and implementation of security controls. Included in this policy is the security classification of data based on the information processed, stored, or transmitted by the system.
2. Security awareness and training policy and procedures which ensures a well-trained workforce is employed as part of a defense-in-depth strategy to protect organizations against a variety of threats targeting or leveraging personnel. Additionally, this policy provides for continuous improvement by the use of course feedback and student skills assessment.
3. Contingency planning policy and procedures which are part of an overall organizational program for achieving continuity of operations for vital mission/business functions.
4. Risk assessment policy and procedures which ensure the locality is effectively measuring and managing risk. Risk tracking, via a Risk Register, and mitigation management, via Plan of Actions and Milestones (POA&Ms) are also required as the risk assessment process.
5. System and services acquisition policy and procedures facilitating the implementation of the system and services acquisition tasks and the associated system and services acquisition controls to mitigate risk associated with those acquisition tasks.
6. Security assessment and authorization policy and procedures which detail how to analyze various levels of risk posed by the localities' IT implementations, and how that risk been accepted as authorized by locality & Department of Elections heads or their designees. This policy also details how residual risk is defined and tracked through mitigation activities.

7. Audit and accountability policy and procedures identify requirements for information security related audit review, analysis, and reporting performed by the locality. Also, reporting and alerting requirements are outlined.
8. Security and Acceptable use (rules of behavior) and disclosure policies and procedures which clearly delineate appropriate use and the limitations and restrictions associated with the use of locality owned information assets, including potential penalties for misuse or policy violations.
9. Personnel Security Management standards establish minimum security standards for localities to develop and implement policies and procedures to minimize the risks associated with personnel management.
10. IT Security Program Management standards establish minimum security standards providing an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.
11. Configuration Management establishes minimum security standards for localities to develop policies and procedures facilitating the implementation of the configuration management policy and the associated configuration management controls.

OPERATIONAL AND TECHNICAL POLICIES AND PROCEDURES

1. Access control policy and procedures which ensure the identification of authorized users and the specification of access privileges. This standard also covers the topics of Least Privilege, Separation of Duties, and Privileged User Management.
2. System and communications protection standards seek to develop procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls. Boundary protection, cryptography, and peripheral device access standards are covered in detail.
3. Incident response minimum standards which the localities to develop, document, and disseminate to localities an incident response policy addressing purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
4. Media protection policy and procedures which address media access, marking, storage, destruction/sanitization, and transport security.
5. Physical and environmental protection policies and procedures which outline requirements for the locality's facility access and environmental protection controls. Power, locations, and temperature/humidity controls are discussed in detail.
6. Password Management Policy establishes minimum security standards for localities to develop policies and procedures minimizing the risk posed by password management practices within the locality's voting system(s). Also covered in detail are password composition and administration/management.
7. System and Information Integrity standard establishes minimum security standards for localities to develop procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls. This standard also details requirements around malicious code, security alerts, and system monitoring.

8. Physical Access and Security establishes minimum security standards for localities to develop procedures to facilitate the implementation of physical access and security policy and the associated physical controls.
9. Maintenance standard establishes minimum security standards for localities to develop procedures facilitating the implementation of the system maintenance policy and the associated system maintenance controls.

COMPLIANCE AND AUDIT

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

SECURITY AND ACCEPTABLE USE MINIMUM SECURITY STANDARD

PURPOSE

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

SCOPE

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

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

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

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

ROLES & RESPONSIBILITIES

- The Department of Elections standing advisory group (per HB2178; pursuant to subsection A of § 24.2-410.2 of the Code of Virginia) is responsible for the review, update and revision of this security standard and related standards on an annual basis or more frequently if needed.
- The locality Electoral Board is accountable and the locality Information Security Officer (ISO) or responsible party is responsible for adherence to this standard and documenting non-compliance via Department of Elections' exception handling.

- Users are responsible and accountable to comply; *any violation may result in administrative and/or disciplinary action.*
- Users are responsible to report any suspicious activity.
- Upon last working day before leaving, users are required to return all property or resources provided to them during their employment/contract/volunteer period.
- The locality ISO or responsible party is responsible for review, update and revision of this standard's procedures on an annual basis or more frequently if needed.

ACCEPTABLE USE

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

UNACCEPTABLE BEHAVIOR

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

PRIVACY AND SHARING SENSITIVE INFORMATION

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

CONNECTING TO NETWORK ASSETS

1. Use only authorized remote connections to connect.

2. Unauthorized installing of software is prohibited.
3. Recommendation: Connection to network assets are made via the network authentication mechanism (Active Directory, LDAP, etc.) instead of local accounts in component Access Control Lists (ACLs). Preferably, individual network accounts are placed in network Group Accounts. The Group Accounts are role based (system ZXY Admin, Power User, etc.).
4. Recommendation: The locality has technologies in place to detect failed network logon attempts. Localities have processes to investigate and escalate (if necessary) logon attempts flagged by the system(s).
5. Recommendation: Localities logically (and physically if possible) segment Guest Wireless segments off from any networks that are used to connect to sensitive elections related system(s). Only pre-registered/approved wireless devices are allowed inside the sensitive elections related system/enterprise network. Guest Wireless devices have no access to any elections related system component devices.
6. Recommendation: Public access to sensitive elections related system “Public” information should only be available via a DMZ architecture segmented off the interior elections related system/enterprise network.

PERSONNEL SANCTION

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

Determination of General Cost Estimates - SAMPLING

Function	Risk Priority	A		B		C		D		E		F		G		H		I	
		CapEx (One Time Qualifying Costs)	OpEx (Ongoing Annual Costs)	CapEx (One Time Qualifying Costs)	OpEx (Ongoing Annual Costs)	CapEx (One Time Qualifying Costs)	OpEx (Ongoing Annual Costs)	CapEx (One Time Qualifying Costs)	OpEx (Ongoing Annual Costs)	CapEx (One Time Qualifying Costs)	OpEx (Ongoing Annual Costs)	CapEx (One Time Qualifying Costs)	OpEx (Ongoing Annual Costs)	CapEx (One Time Qualifying Costs)	OpEx (Ongoing Annual Costs)	CapEx (One Time Qualifying Costs)	OpEx (Ongoing Annual Costs)	CapEx (One Time Qualifying Costs)	OpEx (Ongoing Annual Costs)
Protect	C	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$100	$0	$0	$0	$100,252	$12,000
ID/PR	C	$55,000	$0	$0	$0	$15,000	$0	$0	$15,287	$0	$173,036	$0	$23,115	$1,500	$1,000	$4,000	$14,500	$28,000	$5,600
PR/DE	C	$0	$35,000	$5,000	$1,300	$27,200	$28,580	$0	$0	$115,000	$36,151	$504,134	$4,600	$3,000	$1,000	$0	$20,500	$34,000	$3,200
ALL	C	$15,000	$14,300	$0	$0	$12,000	$8,000	$0	$15,287	$0	$14,801	$0	$29,300	$3,000	$2,000	$0	$29,200	$0	$0
PR/DE	C	$0	$14,300	$0	$0	$0	$13,787	$0	$13,888	$0	$20,700	$0	$10,100	$0	$500	$0	$47,800	$0	$10,000
ID/PR	C	$0	$28,600	$0	$20,000	$0	$21,287	$0	$0	$0	$118,411	$0	$46,000	$0	$25,000	$7,500	$34,600	$12,000	$2,400
Protect	L	$0	$0	$0	$0	$0	$0	$0	$17,987	$0	$0	$0	$2,300	$1,000	$0	$0	$34,500	$0	$0
Protect	M	$30,000	$14,300	$0	$35,000	$0	$40,150	$0	$24,932	$0	$175,903	$0	$31,625	$2,000	$1,500	$7,500	$11,200	$8,000	$1,200
PR/DE	C	$0	$0	$0	$10,000	$0	$10,787	$0	$0	$0	$7,401	$0	$0	$500	$250	$0	$34,300	$12,012	$11,981
ID/PR	H	$7,200	$0	$0	$35,000	$0	$8,787	$0	$0	$0	$233,213	$252,400	$10,100	$0	$0	$10,000	$18,600	$0	$0
PR/DE	H	$25,000	$5,000	$15,000	$1,000	$5,000	$8,787	$30,000	$5,522	$158,125	$21,514	$10,000	$9,000	$4,000	$500	$11,500	$7,400	$0	$4,500
Protect	H	$3,600	$0	$8,600	$2,900	$0	$8,787	$0	$2,821	$0	$29,603	$0	$0	$0	$0	$0	$13,000	$0	$0
ID/PR	H	$22,500	$14,300	$0	$0	$0	$120,000	$0	$27,753	$0	$118,411	$0	$40,250	$500	$500	$0	$146,400	$22,000	$4,400
Protect	H	$1,800	$0	$2,000	$750	$0	$8,787	$0	$3,472	$0	$13,425	$0	$10,100	$800	$500	$200	$11,800	$0	$4,200
Protect	H	$0	$0	$3,000	$500	$75,000		$0	$0	$34,500	$0	$0	$0	$5,000	$500	$1,000	$12,000	$0	$6,300
ALL	H	$60,000	$11,900	$8,600	$2,900	$20,000	$0	$0	$27,753	$0	$29,603	$0	$20,125	$0	$12,500	$0	$11,500	$3,400	$0
PR/DE/RS	L	$7,200	$35,700	$0	$35,000	$0	$109,250	$0	$48,851	$0	$84,228	$0	$5,800	$0	$0	$0	$11,800	$0	$6,000
Protect	H	$0	$0	$12,000	$3,600	$0	$98,137	$0	$8,994	$0	$29,603	$0	$20,100	$0	$500	$0	$13,000	$0	$0
Protect	H	$0	$0	$0	$0	$0	$35,150	$0	$22,231	$0	$122,203	$0	$26,400	$0	$1,000	$0	$7,400	$0	$26,000
ALL	H	$30,000	$14,300	$10,000	$2,000	$6,000	$0	$0	$8,343	$7,401	$0	$5,700	$0	$0	$0	$0	$0	$2,200	$0
ALL	L	$0	$0	$0	$0	$21,275	$15,000	$21,275	$8,994	$21,275	$14,375	$40,000	$15,000	$0	$3,000	$0	$0	$2,200	$0
		$257,300	**$187,700**	**$64,200**	**$149,950**	**$181,475**	**$535,276**	**$51,275**	**$252,115**	**$336,301**	**$1,242,579**	**$812,234**	**$303,915**	**$21,400**	**$50,250**	**$41,700**	**$479,500**	**$224,064**	**$97,781**

Average CapEX	**$ 221,105**
Average OpEx	**$ 366,563**