Wisconsin Elections Commission

Meeting of the Commission
Friday, March 2, 2018
9:00 A.M.

Agenda
Open Session

Teleconference Meeting

Wisconsin Elections Commission Offices
212 E. Washington Avenue, Third Floor
Madison, Wisconsin

A. Call to Order

B. Report of Appropriate Meeting Notice

C. Public Comments

D. Commission Administrator Appointment/Tabled Motion **3**

E. Elections Security Update **8**

F. Voter List Maintenance **13**

G. Approval of Accountant Services Contract

H. Request for Review of Voting Equipment Software Components **16**

I. Closed Session

1. **Personnel Matter**
2. **Potential Litigation**
3. **Litigation**

19.85 (1) (g)	The Commission may confer with legal counsel concerning litigation strategy.
19.85(1)(c)	The Commission may consider employment, promotion, compensation or performance evaluation data of any public employee over which the governmental body has jurisdiction or exercises responsibility.

The Elections Commission will convene in open session but may move to closed session under Wis. Stat. §§ 19.85 (1)(g) and 19.851, and then reconvene into open session prior to adjournment of this meeting. This notice is intended to inform the public that this meeting will convene in open session, may move to closed session, and then reconvene in open session. Wis. Stat. § 19.85 (2).

WISCONSIN ELECTIONS COMMISSION

212 EAST WASHINGTON AVENUE, 3RD FLOOR
POST OFFICE BOX 7984
MADISON, WI 53707-7984
(608) 261-2028
ELECTIONS@WI.GOV
ELECTIONS.WI.GOV

COMMISSIONERS

BEVERLY R. GILL
JULIE M. GLANCEY
ANN S. JACOBS
JODI JENSEN
DEAN KNUDSON
MARK L. THOMSEN, CHAIR

February 26, 2018

Mr. Mark Thomsen, Chair
Wisconsin Elections Commission

Ms. Ann Jacobs, Vice Chair
Wisconsin Elections Commission

Ms. Jodi Jensen
Wisconsin Elections Commission

Mr. Dean Knudson
Wisconsin Elections Commission

Ms. Julie Glancey
Wisconsin Elections Commission

Ms. Beverly Gill
Wisconsin Elections Commission

Dear Commissioners:

After much deliberation regarding the critical work ahead for the Elections Commission as well as my professional future, I have decided to cease pursuing my continued appointment as Administrator. In order to remove any doubt and further controversy regarding the Administrator position, and to preserve the Commission's ability to choose its own Administrator, I am requesting that the Commission appoint another individual to the position. In the short term, I plan to continue to work at the agency as Staff Counsel.

As you know, on January 23, 2018, the State Senate voted to not confirm my appointment as the first Administrator of the Wisconsin Elections Commission. The vote occurred more than 19 months after the Commission's appointment, and despite the success and accomplishments of agency staff and despite the fact that I had no substantive role in the activities of the Government Accountability Board which some legislators objected to. The lack of any credible criticism of my work and the work of the Commission illustrated the folly of the Senate's vote.

Since its inception, the Commission has successfully administered five regular statewide elections, completed the only statewide recount of the 2016 Presidential contest, revamped agency IT applications, developed an enhanced and comprehensive election security plan, conducted testing campaigns for new voting equipment, implemented new laws, and continued its many training initiatives for local election officials. The WEC's program successes also have occurred during the challenge of the agency's transition and further reductions in the level of agency staffing. Rather than celebrating that success and taking credit for it, some have focused on settling scores with imaginary ghosts of the Government Accountability Board. My appointment was a casualty of that obsession. Even in the heat of the Senate's debate, the justification for rejecting my appointment was vague assertions of "no confidence" rather than any specific action I had taken or decision I made, either at the G.A.B. or the WEC.

Obviously, I strongly disagree with the Senate vote. I am proud of what we have achieved at the WEC and what we have in the works. But the reality is that the Senate's action has created a major distraction and an untenable situation for the Commission. The Department of Administration has determined that I must either take an unpaid leave of absence or return to my original classified position of Staff Counsel which I held at the G.A.B. While our agency operations have been consistent with the Commission's decision to continue my appointment, the Senate's action has created some uncertainty for other state agencies that interact with our staff. The agency's request of the Joint Finance Committee to restore three staff positions, which is still fewer positions than the Committee supported during the budget process, remains unaddressed, apparently due to the issues regarding the Administrator position. There has even been talk that Joint Finance may seek to either eliminate the agency's Staff Counsel position or convert it to an unclassified position.

It is time for this foolishness to end. We are in the midst of constant election preparation and administration which will continue until the middle of November. With the development of electronic poll books, enhanced election security planning and other initiatives, the agency cannot afford to be distracted by my status and must focus on moving forward.

I recently participated in my first security briefing from the Department of Homeland Security while I was in Washington, D.C. The substance of the presentation and its conclusions were not surprising given what has been made public, but the message was sobering. All of us must take seriously the risks and threats to America's election systems and processes. That includes policymakers and elected officials. To put it bluntly, I am asking our elected and political leaders to wake up to this new reality and take it seriously before we fall dangerously behind in securing the integrity of elections and voter confidence.

This means, first, I encourage the Commission to advocate for the Joint Finance Committee to promptly approve and reinstate the three staff positions which the bipartisan Commission has requested and which were among the five positions cut during the budget process. These positions are essential to our efforts to secure elections and improve their administration. We are running out of time for the positions to be of significant help to the agency, clerks or voters prior to the fall election cycle.

Second, I believe it is important that the Commission ask legislative leaders and the Joint Finance Committee to stop any further attacks on the agency's Staff Counsel position and on Nathan Judnic personally. Attorney Judnic has had an accomplished career with the G.A.B. and the WEC and has been unfairly targeted simply for doing his job as a civil service employee. There is no basis for any type of disciplinary action involving Nate, and I am confident that DOA would agree with that assessment. Nate shoulders an incredible load and performs at a high level in ways that the Legislature has no idea about or appreciation for. His work should be rewarded rather than denigrated.

Third, to encourage stability and to avoid a recurrence of this situation, I encourage the Commission to ask the Senate to promptly support the Commission's appointed Administrator and confirm the appointment as soon as possible. It is discouraging and demoralizing to a high-performing staff to do everything possible to carry out its statutory responsibilities and then see its administrative head summarily dismissed by the Senate for no sound reason, and without even an opportunity for a public hearing to gather testimony to assess the performance of the Commission's appointee and the agency.

Commissioner Knudson has proposed that the Commission appoint Assistant Administrator Meagan Wolfe to the position of Administrator. Meagan has done an excellent job supervising the agency's WisVote and IT staff, and spearheading our election security planning process. She is in the process of obtaining secret clearance from the Department of Homeland Security and she also attended the recent security briefing in Washington, D.C. I support the Commission appointing Meagan to the position of Administrator and I urge the Senate to promptly confirm her appointment to the permanent position in order to ensure stability and continuity in the agency.

Some have urged that I challenge the Senate's action through litigation. I did research that option. Based on the language in the Statutes, there are certainly sound legal arguments that the Senate's action did not create a vacancy, and that the Commission's subsequent action to continue my appointment is valid. But there would certainly be a personal financial cost to pursue a Court determination, and I have my family and my own future to consider.

In the end, I have decided not to spend additional time, effort and resources in the negative environment of litigation. Leaders in our state government have clearly expressed their preference, misguided as it may be, that I not continue as Administrator. Even if I were to prevail, there is also the reality that the Legislature can change the law to clarify how to achieve its preferred outcome. Furthermore, I am concerned that the uncertainty surrounding my role is delaying action on the desperately needed staff positions requested by the Commission. I do not wish for my personal situation to be used as an excuse for not providing the agency with the resources it needs to be successful, and which both parties in the Legislature have agreed are necessary.

Wisconsin has tried three models of election administration since removing that responsibility from the Secretary of State in the 1970s. The common theme in those models has been the nonpartisan nature of the staff. That is an admirable and essential component of statewide election administration.

However, an argument can also be made that over time the agencies have been at a disadvantage in their relationships with the Legislature because there is no statewide elected official with an independent constituency who is responsible for election administration, or who has been willing to step forward to stand up for agency staff. In my view, while there may be no single perfect model to ensure unbiased and effective administration of elections, the way in which elected policymakers and leaders choose to support or not support the agency can have a significant impact on the agency's ability to pursue its mission, regardless of how it is structured. Uninformed criticism of the agency and its staff makes it more difficult to secure the resources necessary to effectively administer elections, and ultimately threatens to reduce the confidence of voters and the public in the integrity of our elections.

Finally, I want to take this opportunity to publicly thank everyone who has made my work in elections so enjoyable and who has supported my efforts and my continued service as Administrator. My work with the G.A.B. and as Administrator of the Elections Commission has been one of the highlights of my professional life. I want to thank all of you as well as former members of the Elections Commission and the Government Accountability Board. Members of both oversight boards have supported me, challenged me to do my best, and inspired all of us as staff to consistently provide excellent customer service and to do great things with limited resources.

I also appreciate my professional mentors in Wisconsin state government and among my colleagues around the country at the state and federal levels, as well as our many partners at the local level, who have accelerated my progress in this very unique field and role. When I worked as a municipal attorney during my career in private law practice, I developed a great respect for the overworked and underappreciated municipal clerks who not only conduct elections in 1853 municipalities but are often the glue that holds together the many functions of local control in Wisconsin. Municipal clerks, in the smallest towns to the largest cities, are dedicated to serving their voters. Similarly, I have learned so much from the county clerks who are essential partners in election administration. While they are elected on a partisan basis, they focus on problem solving, consensus building and even-handed administration of election and voting laws.

I especially wish to express my unending gratitude to my fellow staff members at the WEC. Some of them helped to bring me along as I tried to learn the many aspects of the elections field starting in 2008. Many of us worked together through the intense and extended years of election-related events that were unique in our state's history and in the nation's experience. More recently, I have had the pleasure of participating in the hiring of excellent additions to our team. Whether new or longtime colleagues, I have had the high honor of serving with truly committed and skilled individuals who are a credit to public service and to the State of Wisconsin. I appreciate their support and friendship, and their consistent knack for making me look good.

When I talk to students or others about the elections profession, I often discuss general characteristics that help election officials to be successful. Hopefully we possess a strong curiosity and intellect, sound judgment and flexibility. But it also helps to have broad shoulders, thick skin and emotional stability. I am lucky to have served with so many who have combined those attributes with a commitment to public service and to effective and fair elections. As many have observed – and it is more true now than ever before – election administrators are defenders of democracy. To the extent I have been able to make contributions to that effort, it is largely by reflecting the best of what I have seen in the individual effort and teamwork of those with whom I have shared a career's worth of experiences and memories.

Finally, I want to thank my family, including my parents and my siblings for their support. And I cannot thank my wife, Judene, and our kids, Jocelyn, Dontay, and Beau, enough for their patience with the long hours and spotlight which are often a part of my job and which can also be an inconvenience to our family. Judene personifies kindness, grace, and strength, and the way she reminds me to prioritize those qualities is one of the many reasons that I love and appreciate her.

Assuming that the Commission appoints a new Interim Administrator at its meeting on March 2nd, my immediate plans are to continue to work in the position of Staff Counsel for the short term. That will allow me to assist the new Administrator in the transition of duties and responsibilities. My understanding is that I would have a short period of time to determine whether to exercise my restoration rights to return to the position of Staff Counsel on a permanent basis. Given the fixation of some in the Senate on removing me from agency service, it would likely be a distraction for me to continue in that position. At this time, I do not intend to exercise those restoration rights, and I plan to pursue other professional opportunities in the near future.

I will always be grateful for the opportunity to serve in the unique position of Wisconsin's chief election official, albeit for a relatively brief period of time. It has challenged me to grow, and provided me with

opportunities to work with excellent partners at the federal, state and local levels. My nine-plus years with the state's elections agency have allowed me to combine my skills, expertise and passion to serve the residents of my home state.

The elections field continues to change quickly. Our world includes issues of ballot access, voting rules, increased use of technology, and greater emphasis on cybersecurity and election security. But at the center of it all is our focus on the voter, the voter's experience, and public confidence in the integrity of election results. As others have before me, I have attempted to preserve that focus and trust, and I have the utmost confidence that my colleagues and friends at the Wisconsin Elections Commission will carry on with that tradition and mission.

Thank you for placing your confidence in me by appointing me as Administrator, and for your support of my leadership as well as the work of our entire staff. I wish you and the Commission the very best in meeting the challenges ahead.

Sincerely,

Michael Haas

WISCONSIN ELECTIONS COMMISSION

212 EAST WASHINGTON AVENUE, 3RD FLOOR
POST OFFICE BOX 7984
MADISON, WI 53707-7984
(608) 261-2028
ELECTIONS@WI.GOV
ELECTIONS.WI.GOV

MEMORANDUM

DATE: For the March 2, 2018 Special Commission Meeting

TO: Members, Wisconsin Elections Commission

FROM: Michael Haas

SUBJECT: Elections Security Update

In light of recent media reports, Commission Chair Thomsen requested that staff provide a brief update regarding the agency's election security planning and specifically an overview of the winter meeting of the National Association of State Election Directors (NASED), which Assistant Administrator Meagan Wolfe and I attended from February 17 – l9, 2018. A more complete report regarding our election security planning will be presented to the Commission at its meeting of March 13, 2018.

Attached is the agenda of the NASED Winter Meeting. As you will note, many of the sessions involve some aspect of election security. Presentations were made by representatives of the Department of Homeland Security, The Belfer Center, MS-ISAC, the Center for Internet Security, and the U.S. Election Assistance Commission. Around the time of the conference, several organizations released best practice documents or playbooks which outline guidance for election officials regarding the security of election systems. The NASED conference provided significant resources for Commission staff to review and incorporate, but did not significantly alter the direction of our planning process.

In addition, we attended a special intelligence briefing hosted by the Department of Homeland Security. Representatives of several federal intelligence agencies outlined information which provided context to the incidents of attempted scanning by Russian government actors in 2016 and the communication issues we experienced with Homeland Security last fall. The overall takeaway from the briefing was that election officials need to continue to be vigilant in protecting IT applications and election processes from interference by governmental and nongovernmental actors. This includes the threats to voter confidence posed by influence campaigns which spread misinformation and seek to plant confusion and division, both related to candidates and political issues, as well as the administration of elections.

The briefing also allowed us to interact with federal intelligence officials with whom we have communicated only by email or telephone. It was intended to provide election officials from many states with a baseline understanding of the current intelligence landscape as it relates to elections, as well as an overview of the processes and challenges involved in gathering and effectively communicating intelligence information. The briefing served to further our relationships and communication with our security partners at the federal level.

NASED Winter Meeting – Member Agenda
February 16 – 19, 2018
The Fairmont Hotel, Grand Ballroom II, Washington, DC

Friday, February 16, 2018

4:30 – 6:30pm	Executive Board Meeting, *Decatur Room*

Saturday, February 17, 2018

8:30 – 9:00 am	Breakfast
9:00 – 10:00 am	CLOSED SESSION Regional Meetings
10:00 – 10:30 am	CLOSED SESSION Regional Summaries
10:45 – 11:30 am	Welcome and Call to Order
11:30 – 12:30 pm	Update on the Government Coordinating Council and Other Resources Available to Election Officials • Robert Kolasky, Deputy Under Secretary - National Protection & Programs Directorate, Department of Homeland Security • Sabra Horne, Director - Stakeholder Engagement and Cyber Infrastructure Resilience, Office of Cybersecurity and Communications, Department of Homeland Security
12:30 – 1:15pm	Lunch
1:30 – 3:00 pm	NASS/NASED Joint Session: State and Local Incident Response Playbook Walkthrough, *Ballroom I* • Caitlin Conley, Defending Digital Democracy Project, The Belfer Center • Siobhan Gorman, Director, Brunswick Group
3:00 – 3:15 pm	Break
3:15 – 4:00 pm	MS-ISAC as the Election ISAC • Ben Spear, Senior Intelligence Analyst, MS-ISAC
4:00 – 5:30 pm	CLOSED SESSION • Litigation update: Michelle Tassinari and Keith Ingram • Committee Descriptions and projects: Judd Choate
6:00 – 8:00 pm	President's Reception and installation of NASED officers, *The Colonnade*

Sunday, February 18, 2018

8:30 – 9:00 am	Breakfast
9:00 – 9:15 am	Gavel acceptance: Incoming President Robert Giles
9:15 – 9:45 am	What's New in the Voluntary Voting Systems Guideline (VVSG) 2.0? • Mary Brady, Manager, National Institute of Standards and Technology • Matt Masterson, Chair, U.S. Election Assistance Commission
9:45 – 10:15 am	The Perspective of the Disability Community on the VVSG 2.0 • Michelle Bishop, Head of Voting Rights, National Disability Rights Network • Lou Ann Blake, Deputy Executive Director, Jernigan Institute, National Federation of the Blind
10:15 – 10:30 am	Break
10:30 – 11:15 am	A Handbook for Elections Infrastructure Security • Dr. Michael Garcia, Center for Internet Security
11:15 – 11:45 pm	Update from the Federal Voting Assistance Program • David Beirne, Director, Federal Voting Assistance Program
11:45 – 12:45 pm	Lunch and Presentation of the Election Center's State Award
12:45 – 1:15 pm	U.S. Postal Service Improvements for 2018 • Dan Bentley, Principal Product Management Specialist, U.S. Postal Service • Ron Stroman, Deputy Post Master General, U.S. Postal Service
1:15 – 2:00 pm	U.S. Election Assistance Commission Update • Matt Masterson, Chair • Tom Hicks, Vice-Chair • Christy McCormick, Commissioner
2:00 – 2:15 pm	Break
2:15 – 6:30 pm	CLOSED SESSION: Offsite Briefing • Buses will leave promptly at 2:30 pm for an offsite visit for an Elections Analytical Exchange with the Department of Homeland Security • **Please bring one form of government issued photo ID: REAL ID Compliant driver's license, current U.S. passport, or state government-issued office badge** • 6:30 is the approximate time we will return to the hotel

Tag your social media posts with #NASED18 and follow us on Twitter @NASEDorg

Monday, February 19, 2018

8:30 – 9:00 am	Breakfast
9:00 – 10:00 am	Advances in Post-Election Auditing • Nikki Charlson, Maryland • Dwight Shellman, Colorado • Amber McReynolds, Director of Elections, City and County of Denver
10:00 – 10:30 am	How Does the Associated Press Do It: Election Night Results Reporting • Don Rehill, Director of Election Research and Vote Tabulation, Associated Press
10:30 – 10:45 am	Break
10:45 – 12:30 pm	Update from Our Non-Profit Partners • David Becker, Executive Director, Center for Election Innovation & Research • Monica Crane Childers, Director of Government Services, Democracy Works • Sam Derheimer, Senior Manager, The Pew Charitable Trusts • John Fortier, Director – Democracy Project, Bipartisan Policy Center • Joseph Lorenzo Hall, Chief Technologist, Center for Democracy & Technology • Shane Hamlin, Executive Director, Electronic Registration Information Center • Kamanzi Kalisa, Director – Overseas Voting Initiative, Council of State Governments • Tammy Patrick, Senior Advisor – Elections, Democracy Fund • Charles Stewart, Founding Director, MIT Data and Science Lab
12:30 – 1:30 pm	Lunch

1:30 – 3:00 pm	CLOSED SESSION
	• At members' request, participants on the non-profit panel may be invited to closed session for approximately 15 minutes to provide additional information
	  ○ Shane Hamlin, Executive Director, Electronic Registration Information Center
	  ○ Tammy Patrick, Senior Advisor – Elections, Democracy Fund
	• Discussion of the Digital Millennium Copyright Act exemption
	• Other business

WiFi Network: Fairmont_Meeting
WiFi Password: NASED2018

Tag your social media posts with #NASED18 and follow us on Twitter @NASEDorg

WISCONSIN ELECTIONS COMMISSION

212 EAST WASHINGTON AVENUE, 3RD FLOOR
POST OFFICE BOX 7984
MADISON, WI 53707-7984
(608) 261-2028
ELECTIONS@WI.GOV
ELECTIONS.WI.GOV

COMMISSIONERS

BEVERLY R. GILL
JULIE M. GLANCEY
ANN S. JACOBS
JODI JENSEN
DEAN KNUDSON
MARK L. THOMSEN, CHAIR

MEMORANDUM

DATE: For the Meeting of March 2, 2018

TO: Members, Wisconsin Elections Commission

FROM: Michael Haas
Interim Administrator

Prepared and Presented by:
Sarah Whitt — WisVote IT Lead
Jodi Kitts — WisVote Specialist

SUBJECT: ERIC Movers List Maintenance Mailing Updates

This memo provides updates on the ERIC Movers list maintenance process that Commission staff performed in last 2017 and early 2018, the impacts the list maintenance had on the 2018 Spring Primary, and staff's plans for moving forward for the 2018 Spring Election.

Background

On October 24, 2017, Commission staff identified approximately 340,000 registered voters who appeared to have moved based on data provided by the Electronic Registration Information Center (ERIC). These voters were then mailed a postcard and encouraged to re-register if they had moved, or were given an option to continue their registration at their current address within 30 days if they did not move.

Voters were flagged as having moved either within Wisconsin or outside of Wisconsin. In-state movers were determined based on having a change of address on file with the post office or having their address updated at the Wisconsin DMV more recently than they last registered to vote. Out-of-state movers were determined if the voter had received a driver license or had registered to vote in another state more recently than they last registered in Wisconsin.

On January 9, 2018 Commission staff deactivated the registration of any voters who did not re-register or did not request continuation at their current address within the 30-day period. Approximately 308,000 voters were deactivated as part of the ERIC process. Around 25,000 voters reregistered, and around 6,000 voters requested continuation at their current address. Around 80,000 postcards were returned to clerks as undeliverable.

Impacts on 2018 Spring Primary

On Election Day, WisVote staff began receiving an increased volume of calls from voters and/or local election officials indicating that some voters were not on the poll book who believed they were registered. Researching these individual cases showed that some of these voter registrations had been deactivated as a result of the ERIC mailing even though the voter indicated at the polls that they had not moved. Several voters reported on social media that they had been removed from the poll list and several media outlets picked up the story. Commission staff issued a press release asking voters to contact the Commission if they had not appeared on the poll book but believed they should have. Thus far Commission staff have investigated around 30 voter situations, and approximately 12 of those appeared to be cases where the voter was flagged by ERIC as having moved but the voter indicated they did not. The remaining cases were caused by other issues or involved voters who actually had moved.

Staff is researching all situations where the voter received the ERIC postcard but indicated they have not moved. While situations vary, some similar cases were reported, such as voters co-signing a vehicle loan and having their name added to the vehicle's title, which then updated their customer address in the DMV database. There were also a few cases of changes of address filed with the US Post Office that appear to have been applied to all individuals in a household rather than just the individual that moved. Staff will be forwarding a list of specific voters to DMV to investigate why their addresses were updated at DMV if the voter indicated they had not move.

Proposed Process for 2018 Spring Election

While there are very few concrete examples of ERIC movers being removed from the poll list even though they did not move, Commission staff would like to be as proactive as possible in avoiding issues for the 2018 Spring Election, which generally experiences higher turnout than the Primary. Commission staff proposes a two-step process to help ERIC movers be able to vote more smoothly in the next election.

1. Commission staff will provide municipal clerks with lists of voters who were deactivated as a result of ERIC list maintenance and have not yet re-registered ahead of the April election. Clerks may reach out to those voters ahead of the election to give the voter an additional chance to confirm if they have moved or not, and if not, the clerk may reactivate their registration. Many municipal clerks also have access to other records or other reliable information sources and may be able to proactively determine if the voter moved or not, and may reactivate the registration if they determine the voter did not move.

   Reviewing these pre-election lists will be optional for clerks, as some clerks may have already reviewed their ERIC inactive lists, or the volume of voters may be prohibitive. The intent is to offer clerks the opportunity and the authority to reactivate voters as needed if they did not move. This will reduce the number of potential voter registration issues that may need to be addressed at the polls.

2. Commission staff will prepare Inactive ERIC Mover lists for use at the polling place on Election Day. These lists will include voters who received the ERIC postcard and were deactivated and have not re-registered since the postcard was sent. If a voter does not appear on the regular poll list, election workers will be able to refer to the Inactive ERIC Mover list to determine if the voter is on that list. If the voter is on this list and has not moved, they will be allowed to sign an affirmation that they did not move (similar to the language on the postcard for voters requesting continuation of registration at their current address), and they will be able to vote without having to re-register. Clerks can then provide those specific examples to Commission staff so that the records and cases can be investigated with the DMV.

   This process at the polling place is similar to that used by states which are subject to the National Voter Registration Act, which Wisconsin is not. In those states, before a voter's registration is inactivated as a result of a mailing, the voter's name must continue to appear on the poll list for two election cycles, and cannot be inactivated unless they do not vote in that time period. If the voter does appear at the polls during that time period, their registration is reactivated and they are permitted to vote without registering again.

In addition to the steps above, Commission staff will be sending another mailing in the summer of 2018 to voters who appear to be eligible to register to vote based on data at DMV, but are not currently registered, as it did in the fall of 2016. This mailing will include many of the voters who were previously registered to vote but were deactivated as part of the ERIC list maintenance process. This mailing will encourage voters who are not registered to register to vote before the fall 2018 elections.

Commission staff will continue to work with staff at ERIC as well as with the Wisconsin DMV to identify the causes of any inaccurate data and work towards ensuring that future list maintenance mailings are not mailed to voters who have not moved.

Conclusion and Motion

Commission staff takes very seriously every voter who indicates they did not move but were removed from the poll book. These processes will allow eligible voters to cast a ballot in April without having to take additional administrative steps. Voters who did move will still need to re-register as they always have. These processes will also allow Commission staff to better quantify the number of voters impacted by this process, as well as provide examples that can be investigated by DMV and ERIC to help improve the list maintenance process in the future.

Recommended Motion:

The Elections Commission approves the staff plan described above to handle registrations of Inactive ERIC Movers at the 2018 Spring Election and directs staff to continue to work with ERIC and DMV to improve the data quality for future list maintenance mailings.

WISCONSIN ELECTIONS COMMISSION

212 EAST WASHINGTON AVENUE, 3RD FLOOR
POST OFFICE BOX 7984
MADISON, WI 53707-7984
(608) 261-2028
ELECTIONS@WI.GOV
ELECTIONS.WI.GOV

COMMISSIONERS

BEVERLY R. GILL
JULIE M. GLANCEY
ANN S. JACOBS
JODI JENSEN
DEAN KNUDSON
MARK L. THOMSEN, CHAIR

MEMORANDUM

DATE: For the March 2, 2018 Special Commission Meeting

TO: Members, Wisconsin Elections Commission

FROM: Nathan W. Judnic
Legal Counsel

SUBJECT: Request for Access to Software Components - Update

Since the Commission's last meeting, there have been several developments related to the Jill Stein Campaign software access request.

The following documents are attached, many of which you already been provided under separate cover when they were originally received:

- Letter and attachments dated February 7, 2018 from the Commission to Attorney Mike Cox confirming the Commission's actions at its January 31, 2018 meeting.
- Letter and attachments dated February 7, 2018 from the Commission to Attorney Chris Meuler confirming the Commission's actions at its January 31, 2018 meeting.
- Wisconsin Test Report Version 2 authored by Pro V and V (dated February 12, 2018).
- Document prepared by Commission staff providing the "final" list of software components and associated software versions that are subject to review.
- Letter dated February 15, 2018 from Attorney Chris Meuler to Chair Mark Thomsen related to the Stein Campaign Review Plan.
- Review Plan submitted by the Stein Campaign (dated February 15, 2018).
- Voting equipment vendor's objection letter – from Daniel J. Fischer (counsel for voting equipment vendors) to Chair Mark Thomsen (dated February 26, 2018).

From a procedural standpoint, the Commission staff would recommend at a minimum:

1) The Commission formally adopt Version 2 of the Test Report provided by Pro V and V. There was some minor cleanup regarding a version of software that was reviewed by the testing lab but it was not reflected in Version 1 of the Report. Version 2 fixed that issue and Commission staff would recommend adopting the new version of the report for purposes of any future review.

2) The Commission formally approve the "final" list of software components and associated software versions that will be subject to review. As you recall, there was some concern over which components and versions of software were actually used in the November 2016 General Election. After researching this issue further, the Commission staff is confident that the list attached accurately reflects what is subject to review under the statute.

As you recall, at the January 31, 2018 meeting, the Commission approved the non-disclosure agreement that had been drafted and approved the recommendations contained in the report from Pro V and V (version 1). The Commission also approved the majority of the parameters for the review that were set forth in a staff memorandum. The exception, was the review plan section of the memorandum, and the Commission required the Stein Campaign to file a review plan by February 15, 2018, which it did.

The voting equipment vendors reviewed the plan, and filed an objection. The review plan submitted contains a date of March 5, 2018 as the first day for the Stein Campaign representatives to have initial access to the software components. Given the objection that has been filed, the Commission staff would at a minimum recommend delaying access to software components until the Commission decides how to handle the objection that has been filed.

It is anticipated that representatives from both the voting equipment vendors and the Jill Stein Campaign will be available to answer any questions the Commission may have on this issue at the meeting.

WISCONSIN ELECTIONS COMMISSION

212 EAST WASHINGTON AVENUE, 3RD FLOOR
POST OFFICE BOX 7984
MADISON, WI 53707-7984
(608) 261-2028
ELECTIONS@WI.GOV
ELECTIONS.WI.GOV

COMMISSIONERS

BEVERLY R. GILL
JULIE M. GLANCEY
ANN S. JACOBS
JODI JENSEN
DEAN KNUDSON
MARK L. THOMSEN, CHAIR

Delivered by email to: mike.cox@koleyjessen.com

February 7, 2018

Michael Cox
Koley Jessen P.C., L.L.O
1125 S. 103rd St., Ste. 800
Omaha, NE 68124

Re: Commission Meeting Follow-up

Mike,

Following up on the Commission's January 31, 2018 meeting, I wanted to reach out and make sure that everyone is on the same page regarding next steps in this process. As you are aware, the Commission made decisions related to the software components review request received from the Jill Stein Campaign in late 2016. The Commission was presented with three documents for review: 1) Commission staff memorandum which set forth the "software components review parameters, 2) Confidentiality Non-Disclosure Agreement which individuals must execute prior to being granted access to any software components, 3) Test Report from Pro V&V, Inc. that provided an opinion as to what software components are subject to review under the statute.

After a discussion with the Commission staff and receiving input from both you and the attorneys representing the Jill Stein Campaign, the Commission passed three motions to modify the original recommendations to: direct that an examination plan be developed by the Jill Stein Campaign which includes a reasonable timeframe for review of the software components, and that the plan be submitted by February 15, 2018; and to clarify that only software components that were used in the 2016 General Election will be subject to review, even if the Pro V&V testing and report included software components that were approved in Wisconsin but not actually used to conduct the 2016 General Election. The motions as adopted are as follows:

Motion #1: The Wisconsin Elections Commission, with the exception of the first sentence contained in paragraph 4.a., adopts this memorandum, the Confidentiality Non-Disclosure Agreement (Attachment 1) and the opinion and technical packages code identified in the Pro V & V, Inc. report (Attachment 2), to the extent those technical packages contain software components that were used in the 2016 General Election and therefore subject to review, as its final decision related to the Jill Stein for President request for access to software components under Wis. Stat. § 5.905(4).

Motion #2: Paragraph 4.a. of the memorandum is modified to read: "By no later than the close of business on February 15, 2018, the Recipient shall provide the designated representative(s) of ES&S and

Dominion ("Vendor") and the Commission with a written examination plan concerning the specific details of all examinations to be conducted, including a reasonable timeframe for the review to occur."

Motion #3: Except for the deadline related to the written examination plan as described in amended Paragraph 4.a. of the memorandum, the final decision of the Wisconsin Elections Commission related to the Jill Stein Campaign for President request for access to software components under Wis. Stat. § 5.905(4) is effective March 2, 2018.

Attached please find an amended memorandum reflecting changes directed by the Commission at its January 31, 2018 meeting.

One outstanding issue that must be addressed, is the modified list of software component packages that are subject to review. As indicated in the Pro V&V report, "to err on the side of transparency" the testing lab created packages for all the code they were provided from the escrow company. The test report indicated that the Commission will need to make the final decision on which software packages will be included in the review. The Commission reiterated its reading of the statute that only the software components that were in use for the 2016 General Election would be subject to review. Based on the Commission's review of its internal records on what systems and components were used, the Commission believes the following electronic voting system components are subject to review:

- **Dominion (Sequoia) – Sequoia Insight**
- **Dominion (Premier) – Accuvote-OS**
- **Dominion (Premier) – Accuvote-TSX**
- **Dominion – Image Cast Evolution (ICE)**
- **Dominion – (Sequoia) – Edge**
- **ES&S – iVotronic**
- **ES&S – M100**
- **ES&S – DS200**
- **ES&S – Optech 3PE**
- **ES&S – DS850**

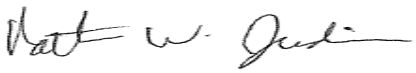
The following software packages are not subject to review, even though they were included in the report from Pro V&V:

- **ES&S – M150-550 (not in use in Wisconsin)**
- **ES&S – M650 (not in use in Wisconsin)**

We will continue to work with you to verify the software versions that were on these systems for use in the 2016 General Election. Once we have verified the software versions in use, the Commission staff will share that information with the Jill Stein Campaign.

If you have any questions on this, please let me know. I can be reached at nathan.judnic@wisconsin.gov or 608-267-0953.

Sincerely,



Nathan W. Judnic
Legal Counsel
Wisconsin Elections Commission

CC: Michael Haas, WEC
Richard Rydecki, WEC

WISCONSIN ELECTIONS COMMISSION

212 EAST WASHINGTON AVENUE, 3RD FLOOR
POST OFFICE BOX 7984
MADISON, WI 53707-7984
(608) 261-2028
ELECTIONS@WI.GOV
ELECTIONS.WI.GOV

ADMINISTRATOR MICHAEL HAAS

COMMISSIONERS

BEVERLY R. GILL
JULIE M. GLANCEY
ANN S. JACOBS
JODI JENSEN
DEAN KNUDSON
MARK L. THOMSEN, CHAIR

MEMORANDUM

DATE: For the January 31, 2018 Special Commission Meeting

TO: Members, Wisconsin Elections Commission

FROM: Michael Haas
Interim Administrator

Prepared and Presented by:
Nathan W. Judnic
Legal Counsel

SUBJECT: Request for Access to Software Components

On December 6, 2016, the Wisconsin Elections Commission ("WEC" or "Commission") received an email from the Jill Stein for President campaign requesting access to the software components that were used to record and tally the votes in the November 2016 General Election pursuant to Wis. Stat. § 5.905(4). Consistent with the statute, the request designated individuals that were authorized to receive access to the software components and requested that any written agreements the designated individuals needed to sign should be provided to the campaign so that access could be granted.

Ultimately, the Commission is the authority charged with making the final decisions as to what software components are reviewed, what agreement is in place to ensure confidentiality of the information reviewed, and what procedures should be in place to facilitate the review.

Since the initial request was received, the Commission staff have had many conversations with both representatives of the Jill Stein campaign and representatives of the two major voting equipment vendors in Wisconsin, Elections Systems & Software ("ES&S") and Dominion Voting Systems, Inc. ("Dominion") to collect information on what these parties believe should be subject to review under the statute, what sort of non-disclosure agreement should be signed prior to access being granted, and what additional parameters that need to be in place to facilitate a review allowed under the statute.

The information received from these parties was extremely helpful in crafting a non-disclosure agreement that comports with the requirements under Wis. Stat. § 5.905(4). Prior to software component access being granted to individuals identified by the Jill Stein campaign, the agreement will need to be executed and filed with the Commission and is included at Attachment 1. The agreement obligates the individuals signing it "to exercise the highest degree of reasonable care to

maintain the confidentiality of all proprietary information to which the person is provided access…" Wis. Stat. § 5.905(4).

The information received from these parties also made it clear, that the Commission staff did not have the in-house technical expertise to advise the Commission on what software components are used to record and tally votes within the complex code of the broad array of systems used in use. The Commission authorized staff to seek technical expertise by utilizing a US E.A.C. certified testing laboratory to review the many lines of code encompassed in these systems and provide an opinion as to what specific software components count and tally votes. The Commission contracted with Pro V & V, Inc. to review the code of equipment manufactured by ES&S and Dominion and provide technical packages of code that meet the statutory definition of what should be subject to review. Essentially, Pro V & V, Inc. was tasked with going through the code and segregating the portions of code that in their opinion counts and tallies votes. In addition to these technical packages of code, Pro V & V, Inc. provided a report detailing the process used to make its determination and a listing of the results. The report issued by Pro V & V, Inc. is included at Attachment 2.

The final decisions for the Commission relate to the parameters and logistics of the actual software components review once an agreement has been signed and access is provided to the individuals identified by the Jill Stein campaign. Again, the information provided by both the Jill Stein campaign and the equipment vendors has been useful in developing reasonable review parameters.

The Commission staff recommends that the Commission adopt the following software components review parameters:

1. Only individuals identified in writing by the Jill Stein for President campaign ("Recipients") shall be granted access to the software components provided by the Commission upon execution of the Confidentiality Non-Disclosure Agreement provided to the individual granted access.

2. Only the software components determined by the Commission to record and tally votes ("software components subject to review") shall be subject to review.

3. The software components review shall take place in a designated secure location selected by the Commission.

4. The software components subject to review shall be made available for review in a secure inspection room under the following conditions:

    a. By no later than the close of business on February 15, 2018~~At least two (2) days prior to any review~~, the Recipient shall provide the designated representative(s) of ES&S and Dominion ("Vendor") and the Commission with a written examination plan concerning the specific details of all examinations to be conducted. Such examination plan shall contain a summary overview of the review intended and thereafter any supplements thereto. Vendor shall be permitted to be present at all times during such examination, but shall not interfere with the review process. An examination plan shall be limited to only those processes that are directly relevant to recording and tallying the votes in Wisconsin. Accordingly, no examination plan shall

include any attempt of copying or reverse engineering of any kind or recompiling of any of the software components subject to review. No examination or procedure may occur that is not identified in the written examination plan unless otherwise agreed upon.

b. The software components subject to review shall at all times remain within the custody, control and oversight of the Commission and access will only be authorized for the duration of the review. All examinations, inspections, analysis, operation, testing or use shall occur solely in secure access-controlled rooms at a facility controlled by the Commission and agreed to by Vendor. The Commission shall select a secure location that will monitor access to and from the examination room. All authorized persons must sign a log-in sheet before entry to the examination room, and the log-in sheet shall be maintained by the Commission's designated representative with a copy provided to Vendor upon request. Vendor shall have the right to request additional reasonable security measures and/or procedures if reasonably necessary to ensure the security of the software components subject to review pursuant to the written examination plan submitted by the Recipient. Vendor shall be afforded a reasonable opportunity to inspect the room for compliance with this Agreement and other reasonable security measures prior to the review commencing. No other use or access is permitted in the examination room until the examination has been completed.

c. The software components subject to review may be encrypted and/or password-protected as considered reasonable by the Vendor. In such instances, the Commission shall keep track of all persons to who it provides corresponding encryption keys and pass codes. A list containing the names of these individuals shall be disclosed to Vendor upon request.

d. The software components subject to review will be loaded on one or more non-networked computer(s) preloaded with software tools agreed to in advance by the parties for use in viewing, searching, and analyzing the software components subject to review; such computer(s) shall be password protected and maintained in a secure, locked area. Use of any input/output device (e.g., USB memory stick, CD, compact flash, portable hard drive, etc.) is prohibited while accessing the computer containing the software components subject to review. After the software components subject to review and software tools for viewing are loaded on the computer, all ports shall be sealed with tamper evident seals. Absent the express written permission of Vendor, the Recipient shall not be permitted to output or record any proprietary information onto any portable, non-portable, or network media, by any means even if such means exist on the computer (including, but not limited to, compact flash, CD-R/RW drive, Ethernet, Internet, e-mail access or USB). No outside electronic devices, or other input/output devices or recording devices, including but not limited to, computers, cellular phones, tablets, cameras, sound recorders, personal digital assistants (PDAs), peripheral equipment, CDs, DVDs, drives of any kind (e.g. hard drives or thumb drives), or other hardware shall be permitted in the secure room. No devices may be connected to the computer(s) containing the software components subject to review or otherwise used to copy or record the software components subject to review from the computer. The computer(s) containing the software components subject to review

will be made available for inspection during regular business hours, upon reasonable notice to Vendor.

e. No person shall reproduce, perform, distribute or prepare works derivative of the software components subject to review, other proprietary information or materials or permit anyone else to do so or to install any works derivative of the same on any computers outside of the confines of the examination room or inapposite the terms of this Agreement. Anyone reviewing the software components shall not tamper with the equipment or software components in any manner whatsoever.

f. The only persons in the examination room at the time of any examination pursuant to the examination plan and this Agreement shall be the Recipient or Recipients, designated members of the Commission staff or individuals designated by the Commission staff and any designated Vendor representatives. No person permitted access to the examination room for any reason shall remove any media, notes, or recordings containing the software components subject to review from the examination room, nor allow access to the room or to the software components subject to review for or by anyone else. The Commission will fully purge and delete the software components subject to review from each computer used at the conclusion of the Review.

g. Any notes taken during the Review may not be literal transcriptions of any of the software components subject to review nor may they be used to prepare literal transcriptions of any of the software components subject to review, but, among other things, may be sufficient to describe the function of any portion thereof.

h. Notes taken during the Review may be retained by Recipient after the Review, provided they do not contain proprietary information. For purposes of notes, upon request, Vendor shall have a reasonable opportunity to review such notes to verify that they do not contain any proprietary information.

i. When not being used, software components subject to review shall be stored in the respective secured, locked examination room pursuant to the terms of the parameters described herein.

j. Reasonable modifications to the parameters described herein may be suggested by the Recipient, Vendor or Commission to facilitate the orderly review of the software components designated, but any suggested modifications only become effective if all parties involve agree to such modifications.

Given the complexity of the issues involved, the Commission staff recommends delaying the effective date of any final decision made by the Commission by 30 days. This “stay” period will allow the Jill Stein for President campaign, ES&S and Dominion to examine the decision and prepare accordingly before any agreements are signed and software components are available for review.

Recommended Motion #1: The Wisconsin Elections Commission, with the exception of the first sentence contained in paragraph 4.a., adopts this memorandum, the Confidentiality Non-Disclosure Agreement (Attachment 1) and the opinion and technical packages of code identified in the Pro V & V, Inc. report (Attachment 2), to the extent those technical packages contain software components that were used in the 2016 General Election and therefore subject to review, as its final decision related to the Jill Stein for President request for access to software components under Wis. Stat. § 5.905(4).

Recommended Motion #2: Paragraph 4.a. of the memorandum is modified to read: "By no later than the close of business on February 15, 2018, the Recipient shall provide the designated representative(s) of ES&S and Dominion ("Vendor") and the Commission with a written examination plan concerning the specific details of all examinations to be conduct, including a reasonable timeframe for the review to occur."

Recommended Motion #3~~2~~: Except for the deadline related to the written examination plan as described in amended Paragraph 4.a. of the memorandum, t~~T~~he final decision of the Wisconsin Elections Commission related to the Jill Stein for President request for access to software components under Wis. Stat. § 5.905(4) is effective March 2, 2018.

WISCONSIN ELECTIONS COMMISSION

212 EAST WASHINGTON AVENUE, 3RD FLOOR
POST OFFICE BOX 7984
MADISON, WI 53707-7984
(608) 261-2028
ELECTIONS@WI.GOV
ELECTIONS.WI.GOV

COMMISSIONERS

BEVERLY R. GILL
JULIE M. GLANCEY
ANN S. JACOBS
JODI JENSEN
DEAN KNUDSON
MARK L. THOMSEN, CHAIR

Delivered by email to: cmm@ffsj.com

February 7, 2018

Christopher M. Meuler
Friebert, Finerty & St. John, S.C.
Two Plaza East – Suite 1250
330 East Kilbourn Ave.
Milwaukee, WI 53202

Re: Commission Meeting Follow-up

Chris,

Following up on the Commission's January 31, 2018 meeting, I wanted to reach out and make sure that everyone is on the same page regarding next steps in this process. As you are aware, the Commission made decisions related to the software components review request received from the Jill Stein Campaign in late 2016. The Commission was presented with three documents for review: 1) Commission staff memorandum which set forth the "software components review parameters, 2) Confidentiality Non-Disclosure Agreement which individuals must execute prior to being granted access to any software components, 3) Test Report from Pro V&V, Inc. that provided an opinion as to what software components are subject to review under the statute.

After a discussion with the Commission staff and receiving input from both you and the attorney representing the voting equipment vendors, the Commission passed three motions to modify the original recommendations to: direct that an examination plan be developed by the Jill Stein Campaign which includes a reasonable timeframe for review of the software components, and that the plan be submitted by February 15, 2018; and to clarify that only software components that were used in the 2016 General Election will be subject to review, even if the Pro V&V testing and report included software components that were approved in Wisconsin but not actually used to conduct the 2016 General Election. The motions as adopted are as follows:

Motion #1: The Wisconsin Elections Commission, with the exception of the first sentence contained in paragraph 4.a., adopts this memorandum, the Confidentiality Non-Disclosure Agreement (Attachment 1) and the opinion and technical packages code identified in the Pro V & V, Inc. report (Attachment 2), to the extent those technical packages contain software components that were used in the 2016 General Election and therefore subject to review, as its final decision related to the Jill Stein for President request for access to software components under Wis. Stat. § 5.905(4).

Motion #2: Paragraph 4.a. of the memorandum is modified to read: "By no later than the close of business on February 15, 2018, the Recipient shall provide the designated representative(s) of ES&S and Dominion ("Vendor") and the Commission with a written examination plan concerning the specific details of all examinations to be conducted, including a reasonable timeframe for the review to occur."

Motion #3: Except for the deadline related to the written examination plan as described in amended Paragraph 4.a. of the memorandum, the final decision of the Wisconsin Elections Commission related to the Jill Stein Campaign for President request for access to software components under Wis. Stat. § 5.905(4) is effective March 2, 2018.

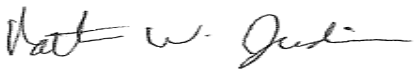
Attached please find an amended memorandum reflecting changes directed by the Commission at its January 31, 2018 meeting.

As directed by the Commission, please compile and submit an examination plan as described in Paragraph 4.a. no later than February 15, 2018. The plan should include a reasonable timeframe for completing the software components review. The plan can be sent directly to me, and I will share it with the Commission and voting equipment vendors once I have received it.

Finally, an outstanding issue that must be addressed, is the modified list of software component packages that are subject to review. As indicated in the Pro V&V report, "to err on the side of transparency" the testing lab created packages for all the code they were provided from the escrow company. The test report indicated that the Commission will need to make the final decision on which software packages will be included in the review. The Commission reiterated its reading of the statute that only the software components that were in use for the 2016 General Election would be subject to review. The Commission staff is still working to confirm the software versions on each piece of equipment that were in use for the 2016 General Election. Once we have confirmed all versions we will pass that information along. I also wanted to inform you that the Commission believes two of the four pieces of equipment listed in the "additional components" portion of Section 2.2 of the Pro V&V report were used in Wisconsin – ES&S – Optech 3PE and ES&S DS850. Therefore, those components are included in the pieces of equipment subject to review under the statute. The ES&S M150-550 and the ES&S M650 were not in use in Wisconsin and therefore are not subject to review under the statute.

If you have any questions on this, please let me know. I can be reached at nathan.judnic@wisconsin.gov or 608-267-0953.

Sincerely,



Nathan W. Judnic
Legal Counsel
Wisconsin Elections Commission

CC: Michael Haas, WEC
Richard Rydecki, WEC

WISCONSIN ELECTIONS COMMISSION

212 EAST WASHINGTON AVENUE, 3RD FLOOR
POST OFFICE BOX 7984
MADISON, WI 53707-7984
(608) 261-2028
ELECTIONS@WI.GOV
ELECTIONS.WI.GOV

ADMINISTRATOR MICHAEL HAAS

COMMISSIONERS

BEVERLY R. GILL
JULIE M. GLANCEY
ANN S. JACOBS
JODI JENSEN
DEAN KNUDSON
MARK L. THOMSEN, CHAIR

MEMORANDUM

DATE: For the January 31, 2018 Special Commission Meeting

TO: Members, Wisconsin Elections Commission

FROM: Michael Haas
Interim Administrator

Prepared and Presented by:
Nathan W. Judnic
Legal Counsel

SUBJECT: Request for Access to Software Components

On December 6, 2016, the Wisconsin Elections Commission ("WEC" or "Commission") received an email from the Jill Stein for President campaign requesting access to the software components that were used to record and tally the votes in the November 2016 General Election pursuant to Wis. Stat. § 5.905(4). Consistent with the statute, the request designated individuals that were authorized to receive access to the software components and requested that any written agreements the designated individuals needed to sign should be provided to the campaign so that access could be granted.

Ultimately, the Commission is the authority charged with making the final decisions as to what software components are reviewed, what agreement is in place to ensure confidentiality of the information reviewed, and what procedures should be in place to facilitate the review.

Since the initial request was received, the Commission staff have had many conversations with both representatives of the Jill Stein campaign and representatives of the two major voting equipment vendors in Wisconsin, Elections Systems & Software ("ES&S") and Dominion Voting Systems, Inc. ("Dominion") to collect information on what these parties believe should be subject to review under the statute, what sort of non-disclosure agreement should be signed prior to access being granted, and what additional parameters that need to be in place to facilitate a review allowed under the statute.

The information received from these parties was extremely helpful in crafting a non-disclosure agreement that comports with the requirements under Wis. Stat. § 5.905(4). Prior to software component access being granted to individuals identified by the Jill Stein campaign, the agreement will need to be executed and filed with the Commission and is included at Attachment 1. The agreement obligates the individuals signing it "to exercise the highest degree of reasonable care to

maintain the confidentiality of all proprietary information to which the person is provided access…" Wis. Stat. § 5.905(4).

The information received from these parties also made it clear, that the Commission staff did not have the in-house technical expertise to advise the Commission on what software components are used to record and tally votes within the complex code of the broad array of systems used in use. The Commission authorized staff to seek technical expertise by utilizing a US E.A.C. certified testing laboratory to review the many lines of code encompassed in these systems and provide an opinion as to what specific software components count and tally votes. The Commission contracted with Pro V & V, Inc. to review the code of equipment manufactured by ES&S and Dominion and provide technical packages of code that meet the statutory definition of what should be subject to review. Essentially, Pro V & V, Inc. was tasked with going through the code and segregating the portions of code that in their opinion counts and tallies votes. In addition to these technical packages of code, Pro V & V, Inc. provided a report detailing the process used to make its determination and a listing of the results. The report issued by Pro V & V, Inc. is included at Attachment 2.

The final decisions for the Commission relate to the parameters and logistics of the actual software components review once an agreement has been signed and access is provided to the individuals identified by the Jill Stein campaign. Again, the information provided by both the Jill Stein campaign and the equipment vendors has been useful in developing reasonable review parameters.

The Commission staff recommends that the Commission adopt the following software components review parameters:

1. Only individuals identified in writing by the Jill Stein for President campaign ("Recipients") shall be granted access to the software components provided by the Commission upon execution of the Confidentiality Non-Disclosure Agreement provided to the individual granted access.

2. Only the software components determined by the Commission to record and tally votes ("software components subject to review") shall be subject to review.

3. The software components review shall take place in a designated secure location selected by the Commission.

4. The software components subject to review shall be made available for review in a secure inspection room under the following conditions:

    a. By no later than the close of business on February 15, 2018~~At least two (2) days prior to any review~~, the Recipient shall provide the designated representative(s) of ES&S and Dominion ("Vendor") and the Commission with a written examination plan concerning the specific details of all examinations to be conducted. Such examination plan shall contain a summary overview of the review intended and thereafter any supplements thereto. Vendor shall be permitted to be present at all times during such examination, but shall not interfere with the review process. An examination plan shall be limited to only those processes that are directly relevant to recording and tallying the votes in Wisconsin. Accordingly, no examination plan shall

include any attempt of copying or reverse engineering of any kind or recompiling of any of the software components subject to review. No examination or procedure may occur that is not identified in the written examination plan unless otherwise agreed upon.

b. The software components subject to review shall at all times remain within the custody, control and oversight of the Commission and access will only be authorized for the duration of the review. All examinations, inspections, analysis, operation, testing or use shall occur solely in secure access-controlled rooms at a facility controlled by the Commission and agreed to by Vendor. The Commission shall select a secure location that will monitor access to and from the examination room. All authorized persons must sign a log-in sheet before entry to the examination room, and the log-in sheet shall be maintained by the Commission's designated representative with a copy provided to Vendor upon request. Vendor shall have the right to request additional reasonable security measures and/or procedures if reasonably necessary to ensure the security of the software components subject to review pursuant to the written examination plan submitted by the Recipient. Vendor shall be afforded a reasonable opportunity to inspect the room for compliance with this Agreement and other reasonable security measures prior to the review commencing. No other use or access is permitted in the examination room until the examination has been completed.

c. The software components subject to review may be encrypted and/or password-protected as considered reasonable by the Vendor. In such instances, the Commission shall keep track of all persons to who it provides corresponding encryption keys and pass codes. A list containing the names of these individuals shall be disclosed to Vendor upon request.

d. The software components subject to review will be loaded on one or more non-networked computer(s) preloaded with software tools agreed to in advance by the parties for use in viewing, searching, and analyzing the software components subject to review; such computer(s) shall be password protected and maintained in a secure, locked area. Use of any input/output device (e.g., USB memory stick, CD, compact flash, portable hard drive, etc.) is prohibited while accessing the computer containing the software components subject to review. After the software components subject to review and software tools for viewing are loaded on the computer, all ports shall be sealed with tamper evident seals. Absent the express written permission of Vendor, the Recipient shall not be permitted to output or record any proprietary information onto any portable, non-portable, or network media, by any means even if such means exist on the computer (including, but not limited to, compact flash, CD-R/RW drive, Ethernet, Internet, e-mail access or USB). No outside electronic devices, or other input/output devices or recording devices, including but not limited to, computers, cellular phones, tablets, cameras, sound recorders, personal digital assistants (PDAs), peripheral equipment, CDs, DVDs, drives of any kind (e.g. hard drives or thumb drives), or other hardware shall be permitted in the secure room. No devices may be connected to the computer(s) containing the software components subject to review or otherwise used to copy or record the software components subject to review from the computer. The computer(s) containing the software components subject to review

will be made available for inspection during regular business hours, upon reasonable notice to Vendor.

e. No person shall reproduce, perform, distribute or prepare works derivative of the software components subject to review, other proprietary information or materials or permit anyone else to do so or to install any works derivative of the same on any computers outside of the confines of the examination room or inapposite the terms of this Agreement. Anyone reviewing the software components shall not tamper with the equipment or software components in any manner whatsoever.

f. The only persons in the examination room at the time of any examination pursuant to the examination plan and this Agreement shall be the Recipient or Recipients, designated members of the Commission staff or individuals designated by the Commission staff and any designated Vendor representatives. No person permitted access to the examination room for any reason shall remove any media, notes, or recordings containing the software components subject to review from the examination room, nor allow access to the room or to the software components subject to review for or by anyone else. The Commission will fully purge and delete the software components subject to review from each computer used at the conclusion of the Review.

g. Any notes taken during the Review may not be literal transcriptions of any of the software components subject to review nor may they be used to prepare literal transcriptions of any of the software components subject to review, but, among other things, may be sufficient to describe the function of any portion thereof.

h. Notes taken during the Review may be retained by Recipient after the Review, provided they do not contain proprietary information. For purposes of notes, upon request, Vendor shall have a reasonable opportunity to review such notes to verify that they do not contain any proprietary information.

i. When not being used, software components subject to review shall be stored in the respective secured, locked examination room pursuant to the terms of the parameters described herein.

j. Reasonable modifications to the parameters described herein may be suggested by the Recipient, Vendor or Commission to facilitate the orderly review of the software components designated, but any suggested modifications only become effective if all parties involve agree to such modifications.

Given the complexity of the issues involved, the Commission staff recommends delaying the effective date of any final decision made by the Commission by 30 days. This “stay” period will allow the Jill Stein for President campaign, ES&S and Dominion to examine the decision and prepare accordingly before any agreements are signed and software components are available for review.

Recommended Motion #1: The Wisconsin Elections Commission, with the exception of the first sentence contained in paragraph 4.a., adopts this memorandum, the Confidentiality Non-Disclosure Agreement (Attachment 1) and the opinion and technical packages of code identified in the Pro V & V, Inc. report (Attachment 2), to the extent those technical packages contain software components that were used in the 2016 General Election and therefore subject to review, as its final decision related to the Jill Stein for President request for access to software components under Wis. Stat. § 5.905(4).

Recommended Motion #2: Paragraph 4.a. of the memorandum is modified to read: "By no later than the close of business on February 15, 2018, the Recipient shall provide the designated representative(s) of ES&S and Dominion ("Vendor") and the Commission with a written examination plan concerning the specific details of all examinations to be conduct, including a reasonable timeframe for the review to occur."

Recommended Motion #3~~2~~: Except for the deadline related to the written examination plan as described in amended Paragraph 4.a. of the memorandum, t~~T~~he final decision of the Wisconsin Elections Commission related to the Jill Stein for President request for access to software components under Wis. Stat. § 5.905(4) is effective March 2, 2018.

Test Report

Software Component Review Report for the State of Wisconsin

Prepared by: Jack Cobb

Jack Cobb, Laboratory Director

February 12, 2018

v. TR-01-04-WIS-2017-01.02

1 Introduction

The purpose of this Test Report is to document the procedures that Pro V&V, Inc. followed to perform software component review on certified systems in the state of Wisconsin. Pro V&V performed this effort with the intent of providing professional and technical services for review of the software components of electronic voting systems used in the State of Wisconsin and determine which components are necessary to record and tally votes in an election.

1.1 References

The documents listed below were utilized in the development of this Test Report:

- Wisconsin Software Component Verification
- Wisconsin Elections Commission Contract for Software Component Review Services

1.2 Terms and Abbreviations

The terms and abbreviations applicable to the development of this Test Report are listed below:

EAC – Election Assistance Commission

TDP – Technical Data Package

USB – Universal Serial Bus

VSTL – Voting Systems Test Laboratory

WEC – Wisconsin Elections Commission

1.3 Background

Per Wisconsin Statute § 5.905(4), if a valid petition for a recount is filed under Wisconsin Statute § 9.01 *"in an election at which an electronic voting system was used to record and tally the votes cast, each party to the recount may designate one or more persons who are authorized to receive access to the software components that were used to record and tally the votes in the election."* A valid request from a party to the recount was received by the Wisconsin Elections Commission (WEC). WEC contracted Pro V&V to perform an analysis of the certified systems for use in Wisconsin to determine which components are necessary to record and tally votes in an election.

2 Review Overview

WEC submitted an encrypted USB drive with all voting systems in use in Wisconsin during the 2016 Presidential Election. Pro V&V was able to extract the individual source code repositories for the certified systems.

2.1 Review Materials

The encrypted USB drive contained the following directories:

Dominion Voting System

2006-11-03\WI 2006-10-31 Escrow Deposit – Recount.zip
2006-11-03\WI 2006-10-31 Escrow Deposit.zip
2014-06-04\GEMS 1-18-24D.exe
2015-09-16\Account-9974ML-SBLic01-UID-841-ID-7924\ADJ_2-4-1-3201_ObjectCode_UserDocs.zip
2015-09-16\Account-9974ML-SBLic01-UID-841-ID-7924\ADJ_2-4-1-3201_SourceCode_TechDocs.zip
2015-09-16\Account-9974ML-SBLic01-UID-841-ID-7924\ICC_4-14-17_ObjectCode_UserDocs.zip
2015-09-16\Account-9974ML-SBLic01-UID-841-ID-7924\ICC_4-14-17_SourceCode_TechDocs.zip
2015-09-16\Account-9974ML-SBLic01-UID-841-ID-7924\ICE-4-14-21_ObjectCode_UserDocs.zip
2015-09-16\Account-9974ML-SBLic01-UID-841-ID-7924\ICE-4-14-21_SourceCode_TechDocs.zip
2015-09-16\Account-9974ML-SBLic01-UID-841-ID-7924\ICL_2-1-1-5301_ObjectCode_UserDocs.zip
2015-09-16\Account-9974ML-SBLic01-UID-841-ID-7924\ICL_2-1-1-5301_SourceCode_TechDocs.zip
2015-09-16\Account-9974ML-SBLic01-UID-841-ID-7924\ICP_4-14-17_ObjectCode_UserDocs.zip
2015-09-16\EMS_4-14-37_ObjectCode_UserDocs.zip

Election Systems & Software

2006-11-03\Unity 3.0.1.0 for Wisconsin (Executables and Doc)
2006-11-03\Unity 3.0.1.0 for Wisconsin (Source)
2012-10-23\Unity 3.2.0.0 Revision 3 TDP.exe
2012-10-23\Unity 3.2.0.0 Revision 3 Trusted Build.exe
2013-04-04\Unity 3.4.0.0 TDP.exe
2013-04-04\Unity 3.4.0.0 TrustedBuild.exe
2013-04-04\Unity 3.4.0.0ProductVersionList.xlsx.exe
2013-09-09\TDP.exe
2013-09-09\Trusted Builds.exe

2014-09-17\ A – Disk 1 of 4

2014-09-17\ A – Disk 2 of 4

2014-09-17\ A – Disk 3 of 4

2014-09-17\ A – Disk 4 of 4

2014-09-17\ B – Disk 1 of 4

2014-09-17\ B – Disk 2 of 4

2014-09-17\ B – Disk 3 of 4

2014-09-17\ B – Disk 4 of 4

2015-09-29\ProductInstalls.exe

2015-09-29\SourceOnlyStaging.exe

2015-09-29\TDP.exe

2015-09-29\Unity3.4.1.0WisconsinProductVersionList

2.2 Review Candidate

Per the contract, the electronic voting systems components that were subject to review were the following:

- Dominion (Sequoia) – Sequoia Insight
- Dominion (Premier) – Accuvote-OS
- Dominion(Premier) – Accuvote-TSX
- Dominion – Image Cast Evolution (ICE)
- Dominion (Sequoia) –Edge
- ES&S – iVotronic
- ES&S – M100
- ES&S - DS200

In addition to these components, the encrypted drive had additional components that may be fielded in Wisconsin. These components were added to err on the side of transparency. WEC will need to make a determination on including these components in the final package. The additional components are as listed below:

- ES&S - Optech 3PE
- ES&S - M150-550
- ES&S - M650
- ES&S - DS850

2.3 Review Support Equipment/Materials

In addition to the component source code, the encrypted drive contained the TDP for each system. Pro V&V utilized the TDP when necessary to determine if a component was utilized to "record and tally" votes.

3 Review Process and Results

The following sections outline the process that was followed to evaluate the review candidate defined in Section 2.2.

3.1 General Information

The encrypted USB drive was copied to Pro V&V's network attached storage application. Each directory was extracted and decrypted to a level where no directory contained a compressed or encrypted file.

3.2 Review Procedures

Once Pro V&V had the raw source code files, a manual review of the submitted source code was performed to determine if a component did "record and tally" votes. If a component was determined to "record and tally" votes the entire source code package was moved into a deliverables directory. If a component was determined not to "record and tally" votes it was not copied to the deliverable directory. Pro V&V researched the component versions and structured the deliverables directory in a manner that the component could be traced to the voting system that it is certified with. The final results of this review are noted in Section 3.3.

3.3 Review Results

Below are the voting system name, the component name and version, the associated file name and the SHA256 value for the file:

Unity 3.4.1.0

DS200 1.7.0.0n

source.iso - a3ca2615a25edf7968844223e1cb80f86f48ae4e7df7044824da09c26fe44dc7

M100 5.4.4.5.3

source.tar - 463ef1d77790479bf6be92efafbc6a095b79687a81fc7f1e4d2ba32828f95b72

EVS 5.2.0.0

DS200 2.12.0.0l

source.iso - 4828e1b5159aa8efbbf4b75e5e2b945aa328a2013ebcb675638f8699cd6e5b6a

DS850 2.10.0.0i

source.iso - 8c08f7794c084ce90a12c05deb7a3463fcc52d1ce21415af4bf3b446e10c7a06

EVS 5.3.0.0

DS200 2.13.0.0b

source.iso - 02fac37cdc0f89c3242a89df466355cfffd4303779dffe03a66839da61b70a88

DS850 2.10.0.0i

source.iso - 8c08f7794c084ce90a12c05deb7a3463fcc52d1ce21415af4bf3b446e10c7a06

Unity 3.4.0.1

DS200 V1.6.0.0

DS200 - 1.6.0.0t

COTS.iso - a2630435fcfa67a88c891f122bb1e0fea814702976e15cf2e34bcac6f7441a2b

Doc.iso - 0a8341346642962bc8c44185a17c8246f034a12b10f0607061638d331bb32205

source.iso - e858d4be5f40dfc86c21bb1181f100f44c11344a9406b9c748312aaaf1d2c033

Unity 3.2.1.0

CB_PEB_1.0.2.0a_Source.zip - 39177b2bf7461ae0fd9d6d9777320cb8144f6517b59c930dfa9e154800a16968

CB_M100_1.4.1.0a_Source.zip - b46b017c0ceb6765f542e03deacabd108adbc3f70e6c4afb02b74ae3ddb4bd80

CB_650_1.2.1.0a_Source.zip - 5bce9d7da618d3aefb904be79aeb8ccce68e042ee01048ab54fd513724041365

CB_EAGL_1.3.2.0a_Source.zip - 84070e97289a92eb938ef6a04f4a7fdfaf05f1245c68ba9ca3e9cb9b2ad91b9b

Unity 3.4.0.0

DS200 - 1.6.1.0l

COTS.iso - d609c9735b08540714b8609815414648621235 0d391b0227a248844cf37b2015

Doc.iso - 0b5f6e6dd84e43ebc523dbe375ce2f208c9ee9bed00dbb1c5f0c749906dd1367

source.iso - 39599ddbab7a1fafb60b068e789fb98a118726c4ca97bac0947c4c776e09c2b6

Unity 3.2.0.0

CB_M100_1.4.1.0a_Source.zip - b46b017c0ceb6765f542e03deacabd108adbc3f70e6c4afb02b74ae3ddb4bd80

CB_650_1.2.1.0a_Source.zip - 5bce9d7da618d3aefb904be79aeb8ccce68e042ee01048ab54fd513724041365

CB_EAGL_1.3.2.0a_Source.zip - 84070e97289a92eb938ef6a04f4a7fdfaf05f1245c68ba9ca3e9cb9b2ad91b9b

M650 2.2.2.0.1

M650_2.2.2.0.1_Source.tar - 8f3e1f4419594b84d6cb91931304ac6e8b5c6549130c10e0dc58e823371507ad

Unity 3.2.0.0 rev 3

DS200 - 1.6.1.0l

COTS.iso - d609c9735b08540714b8609815414648621235 0d391b0227a248844cf37b2015

Doc.iso - 0b5f6e6dd84e43ebc523dbe375ce2f208c9ee9bed00dbb1c5f0c749906dd1367

source.iso - 39599ddbab7a1fafb60b068e789fb98a118726c4ca97bac0947c4c776e09c2b6

Unity 3.0.1.0

Optech 3PE

Eagle APS 1.50.zip53e46ce855143ae800c49a2f0271de4f243ea70edf1e54c5f00a576497c35c55

Eagle CPS 1.02.zip - d22d81d8ebb77590744b831639629e9f00a2cc136cf3042e0a796e0c658fe59e

Eagle HPS 1.28.zip -7002b732a784359d188789a0893772d41a7a3f6e5c662759ea09d9b542835884

iVotronic 9.1.4.0

V9140-source.zip - 5adb3039a105b5f1faaed20d755579aa0077abab9d8fac87e50ab3309692d133

M100 5.2.0.0

pbc5_2_0_0_15_src.tar.gz - 0bfdfad53e9c7b886e7cd934c5d8eb4d7fe9d04e4526282fe11d141b99f2c55b

M150-550 2.1.2.0
Source
SER30M.ASM - ceb057779a8b198d46952bfdece265fb4983cad24b305151b1a79fd4e9acb83a

M650 2.1.0.0
M650 Display 2.1.0.0.zip - dda92146d6a464fe47af3eeb7c80a5fd89785cb9377406ebc0f7ff81fc7ab54a
M650 Firmware 2.1.0.0.zip - 2b27f7dcb73bcdd216a5cd6698e964057f2bed81cc512f04efe9631f76e5c3e2
M650 Support Scripts 2.1.0.0.zip -63a367a0fbde68d09c3866bc1191e673e575477e27d23a46645de2abf9fc32ee

WinEDS 3.1.012
AVC Edge Firmware Version 5.0.24 Source Code\
CD - Source Code.zip - 7c3dbe9bd08a5d36805f9f28e70cc4265e2394e1bd841e9010a4e590de05688f
Optech Insight\
Source Code.zip - 756b94cb1d1bd006f0d909dd0b3d05d6bd9c6b8c936deef51b916be3ac8ab500

GEMS 1-18-24D
AV-OS PC 1-96-6.zip - 2a82be00159ac7223cafefaf0407e7c67f760478941f17be3e7d88dc0f7fb6de
AV-TSX.zip -0325ea1ee417fab61ba7cc6a9e2ab6a30f6b1791b6ca378912568b8ba8b1db9a

DVS 4.14
ICP_4-14-17_ObjectCode_UserDocs.zip - f1f82dea3c01601b809ffc0d77a45c9e4bb6c09137e28693f46d6f632772ab45
ICE_4-14-21_SourceCode_TechDocs.zip - 871acbbcc28d9a535db188f8ef6c4acaaa0416162db49c92627c6aa0c97283a9
ICC_4-14-17_SourceCode_TechDocs.zip - 81e0313dc81f106a649e731250e69d4a61db04cce5ef68927b85550fd23af199

4 Conclusion

Based upon the review of the components, the final results identified in section 3.3 of this report were determined by Pro V&V as the necessary components of these systems for purposes of recording and tallying votes. The final results have been segregated into an encrypted deliverable and will be provided to WEC as requested so that when access to review software components under Wisconsin Statute § 5.905 (4) is requested, the State of Wisconsin will be confident they are providing what is allowable under the statute.

Software Components Subject to Review per Wis. Stat. § 5.905(4)

-2016 General Election-

Unity 3.0.1.0
MlOO v. 5.2.0.0
iVotronic v. 9.1.4.0
Optech 3PE v. 1.28/1.5.0/1.02

Unity 3.2.0.0 (Rev. 3)
DS200 V. 1.6.1.0

Unity 3.4.0.0
DS200 V. 1.6.1.0

Unity 3.4.0.1
DS200 V. 1.6.1.0

Unity 3.4.1.0
MlOO V. 5.4.4.5
DS200 V. 1.7.0.0

EVS 5.2.0.0
DS200 V. 2.12.0.0

EVS 5.3.0.0
DS200 V. 2.13.0.0
DS850 V. 2.10.0.0

WinEDS 3.1.012
AVC Edge v. 5.0.24
Optech Insight

GEMS 1-18-24D
Accuvote OS
Accuvote TSX

DVS 4.14
ICE 4-14-21

FRIEBERT, FINERTY & ST. JOHN, S.C.
ATTORNEYS AT LAW
330 East Kilbourn Ave. • Suite 1250 • Milwaukee, Wisconsin 53202
Phone 414-271-0130 • Fax 414-272-8191 • www.ffsj.com

February 15, 2018

VIA EMAIL
Nathan.Judnic@wisconsin.gov
Mark L. Thomsen, Chair
c/o Nathan W. Judnic, Esq.
Wisconsin Elections Commission
212 East Washington Avenue, Third Floor
P.O. Box 7984
Madison, WI 53707-7984

Re: Software Components Review

Dear Mr. Thomsen:

Enclosed is the Jill Stein Campaign's "Plan for Examination of Electronic Voting System Software Used to Record and Tally Votes in the November 2016 General Election in Wisconsin." This Plan is submitted in furtherance of the Stein Campaign's request for software inspection pursuant to Wis. Stat. § 5.905(4).

The plan's proposed dates and timeline assume that there is no court action or appeal of the Election Commission's Final Order effective on March 2, 2018. Should there be an appeal or court action relating to the Order or inspection, the proposed dates would in all likelihood need to be reevaluated.

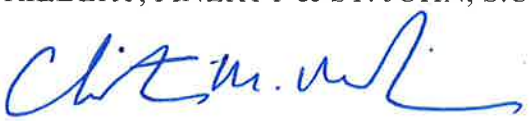
In addition, we submitted a request for a short extension due to timing of receipt of updated information from the WEC as well as a personal matter. The request was denied, but allowed the potential for reasonable modification or amendment, and we preserve our rights in this regard.

Finally, while a significant amount of code is being produced for inspection, the scope of the information being made available appears insufficient under the statute. But, such a determination is better made after the inspection is completed. The Stein Campaign is aware of the 30-day appeal deadline for final orders of an administrative agency. Given the amount of code to review and the logistics involved, the inspection cannot realistically be completed within 30 days of March 2nd. We believe that this issue needs to be addressed and intend to present a formal proposal in the near future that will preserve appeal rights under these circumstances.

Please let us know if there are any questions or if you need additional information. We appreciate the WEC's efforts to date and look forward to commencing the inspection.

Very truly yours,

FRIEBERT, FINERTY & ST. JOHN, S.C.



Christopher M. Meuler
cmm@ffsj.com

CMM/sjf
Enclosure
cc: Matthew D. Brinckerhoff, Esq. – Via Email
Debra L. Greenberger, Esq. – Via Email
David Lebowitz, Esq. – Via Email

Plan for the Examination of Electronic Voting System Software Used to Record and Tally Votes in the November 2016 General Election in Wisconsin

February 15, 2018

Presented on behalf of Dr. Jill Stein

Table of Contents

1. Overview **3**

2. Software Subject to Review **4**

DRE Systems 4

Optical Scan Systems 4

3. Examination Timeline **6**

Phase 1 6

Phase 2 7

Phase 3 7

4. Testing Procedure **9**

5. Test Team Composition **11**

Staffing Level 11

Staff Qualifications 11

6. Materials Required for Testing **12**

1. Overview

Following the November 2016 general election in Wisconsin, presidential candidate Jill Stein successfully petitioned for a statewide recount. That December, Dr. Stein contacted the Wisconsin Elections Commission through counsel to request access to the source code for software components used to record and tally the votes, pursuant to Wis. Stat. § 5.905(4).

On January 31, 2018, the Commission moved to grant access, effective March 2. Under the Commission's order, access will be provided to a list of designated software components. Such access will take place at a facility controlled by the Commission and will be subject to a confidentiality agreement and a series of security requirements designed to protect the confidentiality of proprietary information.

This document describes Dr. Stein's plans for examining the source code.

The examination will be a significant undertaking. Three models of DRE voting machines and eight models of optical scan voting machines were used in Wisconsin during the November 2016 election (see Section 2). For some of these models, multiple software versions were used. The software subject to review is estimated to contain approximately 4 million lines of code.

Accordingly, Dr. Stein plans to conduct the examination in three phases, per the timeline described in Section 3. Following the effective date of the Commission's order, we will conduct a one-day initial code examination on Monday, March 5. This first assessment will assist us in planning further work. We will then hire additional examination team members, procure necessary computer equipment and software, and work with Commission staff to prepare for a week-long round of code review to be conducted in late March. Based on the findings of this first phase, we will make any necessary adjustments to the examination plan and staffing levels and prepare for two subsequent phases of code review, which will take place in April and May.

The examination will apply an election software component testing methodology called Open Ended Vulnerability Testing (OEVT), which we describe in detail in Section 4. OEVT was developed by researchers from the National Institute of Standards and Technology ("NIST") to facilitate the discovery of flaws in voting software architecture, design, and implementation that may not be detected by routine testing and can be exploited to change the outcome of an election. OEVT involves multiple rounds of vulnerability hypothesis generation, refinement, and testing, based on a combination of research and code review.

Dr. Stein takes seriously her responsibility to protect the vendors' proprietary information. The examination team will work in strict adherence to the review security parameters contained in the Commission's order. Team members will be required to sign the non-disclosure agreement provided by the Commission prior to accessing any of the source code under view.

Dr. Stein looks forward to working collaboratively to make this examination as effective as possible. We all share the overarching goal of ensuring that Wisconsin's elections are secure.

2. Software Subject to Review

The Commission determined that three models of DRE voting machines and eight models of optical scanners were used in Wisconsin during the November 2016 general election[1]. For some of these models, multiple software versions were used.

The Commission contracted Pro V & V, Inc. to identify source code that meets the statutory definition of what should be subject to review, pursuant to Wis. Stat. § 5.905(4). For each system used in the election, we list below the software versions and technical packages of source code identified by Pro V & V as subject to review, together with the filenames and corresponding hashes.[2] Pro V & V estimates that the included software totals over 4 million lines of code, written in an array of languages including assembly, C, C++, Java, and COBOL.[3]

Each of the following technical packages of source code will be examined under this plan:

DRE Systems

1. ES&S iVotronic DRE

9.1.4.0 (Unity 3.0.1.0)	
V9140-source.zip	5adb3039a105b5f1faaed20d755579aa0077abab9d8fac87e50ab3309692d133

2. Dominion AVC Edge DRE

5.0.24 (WinEDS 3.1.012)	
AVC Edge Firmware Version 5.0.24 Source Code CD - Source Code.zip	7c3dbe9bd08a5d36805f9f28e70cc4265e2394e1bd841e9010a4e590de05688f

3. Dominion AccuVote TSX DRE

(GEMS 1-18-24D)	
AV-TSX.zip	0325ea1ee417fab61ba7cc6a9e2ab6a30f6b1791b6ca378912568b8ba8b1db9a

Optical Scan Systems

4. ES&S M100 Optical Scanner (2 software versions)

5.4.4.5 (Unity 3.4.1.0)	
source.tar	463ef1d77790479bf6be92efafbc6a095b79687a81fc7f1e4d2ba32828f95b72
5.2.0.0 (Unity 3.0.1.0)	
pbc5_2_0_0_15_src.tar.gz	0bfdfad53e9c7b886e7cd934c5d8eb4d7fe9d04e4526282fe11d141b99f2c55b

[1] Communications from Nathan W. Judnic, Feb. 12 and Feb. 14, 2018.
[2] Pro V & V, Software Component Review Report for the State of Wisconsin, Rev. 2, Feb. 12, 2018.
[3] Communication from Pro V & V, Feb. 12, 2018.

5. ES&S DS200 Optical Scanner (4 software versions)

2.13.0.0 (EVS 5.3.0.0)	
source.iso	02fac37cdc0f89c3242a89df466355cfffd4303779dffe03a66839da61b70a88
2.12.0.0 (EVS 5.2.0.0)	
source.iso	4828e1b5159aa8efbbf4b75e5e2b945aa328a2013ebcb675638f8699cd6e5b6a
1.7.0.0 (Unity 3.4.1.0)	
source.iso	a3ca2615a25edf7968844223e1cb80f86f48ae4e7df7044824da09c26fe44dc7
1.6.1.0 (Unity 3.2.0.0 Rev. 3 and Unity 3.4.0.0 and Unity 3.4.0.1)	
COTS.iso	d609c9735b08540714b8609815414648621235 0d391b0227a248844cf37b2015
Doc.iso	0b5f6e6dd84e43ebc523dbe375ce2f208c9ee9bed00dbb1c5f0c749906dd1367
source.iso	39599ddbab7a1fafb60b068e789fb98a118726c4ca97bac0947c4c776e09c2b6

6. ES&S DS850 Optical Scanner

2.10.0.0 (EVS 5.3.0.0)	
source.iso	8c08f7794c084ce90a12c05deb7a3463fcc52d1ce21415af4bf3b446e10c7a06

7. Dominion Optech IIIP-Eagle Optical Scanner

1.28/1.5.0/1.02 (Unity 3.0.1.0)	
Eagle APS 1.50.zip	53e46ce855143ae800c49a2f0271de4f243ea70edf1e54c5f00a576497c35c55
Eagle CPS 1.02.zip	d22d81d8ebb77590744b831639629e9f00a2cc136cf3042e0a796e0c658fe59e
Eagle HPS 1.28.zip	7002b732a784359d188789a0893772d41a7a3f6e5c662759ea09d9b542835884

8. Dominion Optech Insight Optical Scanner

(WinEDS 3.1.012)	
Source Code.zip	756b94cb1d1bd006f0d909dd0b3d05d6bd9c6b8c936deef51b916be3ac8ab500

9. Dominion ImageCast Evolution Optical Scanner

ICE 4-14-21 (DVS 4.14)	
ICP_4-14-17_ObjectCode_UserDocs.zip	f1f82dea3c01601b809ffc0d77a45c9e4bb6c09137e28693f46d6f632772ab45
ICE_4-14-21_SourceCode_TechDocs.zip	871acbbcc28d9a535db188f8ef6c4acaaa0416162db49c92627c6aa0c97283a9
ICC_4-14-17_SourceCode_TechDocs.zip	81e0313dc81f106a649e731250e69d4a61db04cce5ef68927b85550fd23af199

10. Dominion AccuVote OS Optical Scanner

(GEMS 1-18-24D)	
AV-OS PC 1-96-6.zip	2a82be00159ac7223cafefaf0407e7c67f760478941f17be3e7d88dc0f7fb6de

3. Examination Timeline

Due to the large amount of source code subject to review, and to the requirement that the source code be examined at a facility controlled and designated by the Commission, we plan to conduct the examination in three phases, each centered around a one-week period of on-site code review. The dates below reflect our current proposed dates for examination, subject to staff availability, but in any event our plan contemplates completion of on-site activities within 90 days after the start of the period of on-site review. Segmenting the examination in this manner will allow the examination team to maximize its efficiency during time on site. The intervals between on-site code review will allow us to adjust our test plan, procedures, and staffing levels as necessary.

Primary tasks and proposed dates for each of the phases are described below.

Phase 1

The first phase of the examination will focus on assessing the scope of software under review and identifying and testing the highest-priority software components. Following this phase, we will adjust our test plan, procedures, and staffing level as necessary for Phases 2 and 3.

1.0 Initial Code Review in Wisconsin: **March 5**

We propose to perform initial examination on March 5, the Monday following the effective date of the Commission's order. During this day-long preliminary examination, we will perform initial scoping and assess the quantity and complexity of the code subject to review, which will assist us in planning our full examination.

1.1 Preparation: **March 5–23**

We will bring examination staff under contract (Section 5), plan travel to Wisconsin, acquire necessary documentation, software, and computer equipment (Section 6), and work with Commission staff to prepare the secure examination facilities. The examination team will perform OEVT background research and prepare initial hypotheses to test. We also anticipate spending two days on-site prior to the code review to install computers and software needed for code review.

1.2 Code Review in Wisconsin: **March 26–30**

We propose to conduct the first round of on-site code review over the course of five days, March 26–30. Applying the OEVT methodology, the team will perform manual code review as well as testing using automated bug-finding tools in order to generate and test vulnerability hypotheses.

Phase 2

The examination's second phase will build on the Phase 1 findings to test additional vulnerability hypotheses in the highest-priority software components and extend the scope of testing to additional software components.

2.1 Preparation: **April 2–20**

Preparation will begin in parallel with the previous phase, and will include procurement of additional hardware, software, and documentation that is identified as necessary during the first round of on-site testing. The examination staffing level may also be adjusted based on the scoping performed during Phase 1. The team will use the Phase 1 results, as well as further background research, to develop additional vulnerability hypotheses to test during subsequent code review. We anticipate spending one day on-site prior to the second round of code review in order to prepare additional hardware and software.

2.2 Code Examination in Wisconsin: **April 23–27**

We propose to conduct the second round of on-site code review during April 23–27. The examiners will apply the OEVT methodology to a broader set of the software components. The team will perform further manual code review and automated testing to confirm or refute vulnerability hypotheses and generate further hypotheses for testing in the subsequent phase.

Phase 3

The examination's third and final phase will follow a similar pattern to Phase 2. Building on findings from Phases 1 and 2, the team will complete a final round of OEVT hypothesis generation and testing, including a third week of on-site code review. This phase will extend the scope of testing to any remaining software components.

3.1 Preparation: **April 30–May 18**

3.2 Code Examination in Wisconsin: **May 21–25**

	TASK TITLE	START DATE	DUE DATE	DURATION	PHASE ONE																					
					Mar 5 - 9					Mar 12 - 16					Mar 19 - 23					Mar 26 - 30							
					M	T	W	R	F	M	T	W	R	F	M	T	W	R	F	M	T	W	R	F			
1	**Phase 1**																									
1.0.1	Preliminary on-site code review in Wisconsin for planning and scoping	3/5/2018	3/5/2018	1																						
1.1.0	Finalize team selection and contracting	3/5/2018	3/16/2018	10																						
1.1.1	Additional equipment and software procurement	3/5/2018	3/21/2018	13																						
1.1.2	Deliver and set up equipment in Wisconsin	3/22/2018	3/23/2018	2																						
1.2	On-site code review in Wisconsin	3/26/2018	3/30/2018	5																						

	TASK TITLE	START DATE	DUE DATE	DURATION	PHASE TWO																					
					Apr 2 - 6					Apr 9 - 13					Apr 16 - 20					Apr 23 - 27							
					M	T	W	R	F	M	T	W	R	F	M	T	W	R	F	M	T	W	R	F			
2	**Phase 2**																									
2.1.0	Additional preparation, contracting, and equipment procurement as necessary	4/2/2018	4/19/2018	14																						
2.1.1	Deliver and set up equipment in Wisconsin	4/20/2018	4/20/2018	1																						
2.2	On-site code review in Wisconsin	4/23/2018	4/27/2018	5																						

	TASK TITLE	START DATE	DUE DATE	DURATION	PHASE THREE																					
					Apr 30 - May 4					May 7 - 11					May 14 - 18					May 21 - 25							
					M	T	W	R	F	M	T	W	R	F	M	T	W	R	F	M	T	W	R	F			
3	**Phase 3**																									
3.1.0	Additional preparation, contracting, and equipment procurement as necessary	4/30/2018	5/17/2018	14																						
3.1.1	Deliver and set up equipment in Wisconsin	5/18/2018	5/18/2018	1																						
3.2	On-site code review in Wisconsin	5/21/2018	5/25/2018	5																						

Figure 1: Project Timeline. Shaded columns correspond to dates of on-site work in Wisconsin.

4. Testing Procedure

The examination team will apply a voting system testing methodology called Open Ended Vulnerability Testing (OEVT). OEVT is designed to discover architecture, design, and implementation flaws that may not be detected using systematic functional, reliability, and security testing and can be exploited to change the outcome of an election. OEVT was developed by researchers from the National Institute of Standards and Technology ("NIST") and recommended by the Technical Guidelines Development Committee (TGDC) to the U.S. Election Assistance Commission.[4] Specifically, the examination team will apply the approach NIST calls "OEVT for Individual Voting System Components."
Here we detail the applicable steps of this approach, as adapted from Version 1.3 of NIST's OEVT report:[5]

1. Preparation

a. The team will become familiar with the component architecture and design. The team will perform a high-level security analysis of the component and identify all input interfaces that may be subject to malicious input scenarios.
b. The team will review developer and testing laboratory test documents (if available) to gain insight into the degree of rigor applied. The purpose of this step is to gauge the comprehensiveness of prior testing and use that to identify areas likely to have flaws.
c. The team will become familiar with previous security analysis and penetration testing conducted for the component and for older versions of the component.

2. Code Review

a. The team will perform manual source code review to identify potential issues and develop flaw hypotheses.
b. The team will also use automated code analysis tools to analyze the code for buffer overflows, memory leaks, dead code, and otherwise suspicious code.

3. Hypothesis Generation

a. The team will use its knowledge of the system internals and analysis from the steps above, and its own penetration testing expertise, to hypothesize possible ways to manipulate the system. The hypotheses will be recorded.
b. The team will remove hypotheses whose associated vulnerabilities have been disproved by the developer's testing, by independent laboratory testing, or by previous security analysis and penetration testing.

[4] TGDC, "Voluntary Voting System Guidelines (VVSG) Recommendations to the EAC", August 31, 2007. https://www.nist.gov/itl/voluntary-voting-system-guidelines-vvsg-recommendations-eac-august-31-2007
[5] NIST, "Open Ended Vulnerability Testing for Software Independent Voting Systems", May 16, 2007. https://www.nist.gov/sites/default/files/documents/itl/vote/OEVT.pdf

c. The team will evaluate the flaws hypothesized and flaws proven by previous security analysis and penetration testing activities for the component. The team will add plausible flaws to the set of open hypotheses.
d. The team will identify any known vulnerabilities in subcomponents by searching CVE databases and other available sources. The team will add these vulnerabilities to the list of hypotheses developed above.
e. The team will make a broad search for published vulnerabilities and flaw hypotheses that may be applicable to the voting system. This process will include considering vulnerabilities and hypothesized vulnerabilities in similar systems. The team will add these to the set of flaw hypotheses as applicable.
f. The team will use its knowledge of the system to identify inputs and internal probes that will induce errors that are either externally visible or internally handled by the system but were not exercised by the developer testing or by independent laboratory testing. The team will add these to the flaw hypotheses.
g. The team will identify inputs and internal probes that will invoke code segments that were not exercised by the developer testing or by independent laboratory testing. The team will add these to the flaw hypotheses.
h. The team will assess commercial off-the-shelf software (COTS) used in the component to determine if the COTS security can be bypassed or whether privilege (e.g., administrative access) can otherwise be gained to negate the COTS configuration assumptions on which the voting application security is based. The team will add flaw hypotheses based on the assessment results.

4. Hypothesis Testing

a. The team will evaluate the cumulative hypotheses and reject the ones that are not plausible. The team will prioritize the remaining hypotheses based on payoff potential (damage the flaw can cause if present) and effort involved to test them.
b. The team will take the top vulnerability hypotheses and use further source code examination to help confirm or reject them.
c. Based on the results of 4(b), new hypotheses will be developed and step 4 will be repeated until the set of hypotheses or the examination resources are exhausted.

5. Test Team Composition

Staffing Level

The NIST OEVT study recommends that the test team should plan 9–30 person weeks per voting system, depending on the complexity of the software. To arrive at a preliminary estimate of the staffing level required, we assume that the optical scan systems are of low complexity, requiring 10 person-weeks each, and the DRE systems are of high-complexity, requiring 25-person weeks each, for a total of 145 person-weeks to evaluate all ten systems. We will refine these estimates after examining the software components and assessing their complexity.

System type	Number of systems Subject to test	Estimated person-weeks per system	Person-weeks subtotal
DRE	3	25	75
Optical Scan	7	10	70
Estimated total person-weeks for complete OEVT examination:			**145**

Under the OEVT methodology, only some steps require source code access, so we further estimate that one third of the person-hours will need to be spent working on-site with access to the code. To complete the examination within the three weeks of on-site time called for in our schedule, we will plan for a test team size of approximately 16 people.

We anticipate that the number of participating staff will vary between the three phases. It is likely that fewer staff will take part in Phase 1, due to the relatively short lead time before the on-site code review. We will then adjust the staff level based on the Phase 1 interim findings and any necessary revisions to this test plan.

Staff Qualifications

The team will consist of an examination director and a group of code reviewers. All will have extensive experience and expert qualifications in computer security analysis.

We will provide the names and qualifications of each team member to the Commission at least one week prior to that team member obtaining access to the source code. Only individuals identified in writing by Dr. Stein shall receive access to the software components provided by the Commission, and only upon execution of the Confidentiality Non-Disclosure Agreement provided to the individual by the Commission.

6. Materials Required for Testing

Here we list the computer hardware, software, and other materials that will be required to be available in the designated secure facility in order to conduct the on-site code review. Dr. Stein will work with Commission staff to ensure that these resources are supplied and installed prior to the scheduled code review periods.

This is a preliminary list, and we will update it as preparations for the examination progress.

Necessary Material	**Use During Examination**
Multiple desktop computers and monitors	Reviewing source code, preparing notes (*One per examination staff member; quantity to be determined during Phase 1 preparation.*)
Microsoft Windows 10	Desktop operating system
Microsoft Office	Preparing notes, viewing reports and documentation
Adobe Acrobat Reader	Viewing reports and documentation
Microsoft Visual Studio	Integrated development environment for source code review
Eclipse Desktop	Integrated development environment for source code review
VMWare Workstation 14	VM hypervisor for running Ubuntu
Ubuntu 16.04 LTS with all standard packages	Unix-like operating system with programming, data processing, and text processing tools
[Static analysis software]	Automated code analysis (*Specific software tools to be selected during Phase 1 preparation.*)
Pens, pencils, paper, etc.	Preparing notes
Whiteboard, pens, and erasers	Organization and note taking

In addition to the materials above, we will compile a comprehensive list of documentation that should be available in searchable electronic form within the examination room during on-site code review. The documentation will include at least the following: prior security evaluations, test reports, and certification documents pertaining to the source code subject to review; data sheets and API documentation related to the hardware and software used in the models of machines; technical documentation for the programming languages and libraries in which the software subject to review is written.

KOLEY JESSEN

ATTORNEYS

KOLEY JESSEN PC, LLO
1125 SOUTH 103RD STREET
SUITE 800
OMAHA, NE 68124

PHONE: 402.390.9500
FAX: 402.390.9005

koleyjessen.com

February 26, 2018

VIA E-MAIL NATHAN.JUDNIC@WISCONSIN.GOV

Mark L. Thomsen, Chair
Wisconsin Election Commission
c/o Nathan W. Judnic, Esq.
212 East Washington Avenue, Third Floor
P.O. Box 7984
Madison, WI 53707-7984

Re: Vendors' Objections to Software Components Review
Our File No.1928-261

Dear Chairperson Thomsen and Members of the Wisconsin Election Commission:

As you may recall, our law firm represents Election Systems & Software, LLC, and Dominion Voting Systems, Inc. (individually "ES&S" and "DVS" respectively, and collectively the "Vendors") in relation to the Jill Stein Campaign's (the "Campaign") request to review certain software components of the Vendor's electronic voting systems used in the November 2016 election in Wisconsin. Specifically, the Campaign invokes Wis. Stat. § 5.905, which permits a limited review of just the software components used to "record and tally the votes." At the Commission's hearing on January 31, 2018, the Commission required the Campaign to submit a proposed review plan by February 15 to allow both the Commission and the Vendors to review such plan for compliance with the statute and with the security restrictions and procedures the Commission shall require as compelled by the statute. The Campaign submitted its plan with cover letter late in the day on February 15, entitled "Plan for Examination of Electronic Voting System Software Used to Record and Tally Votes In the November 2016 General Election in Wisconsin" (the "Plan").

The Vendors vehemently object to the Campaign's Plan in its entirety. In short, the Plan grossly exceeds the narrow scope and clear purpose of the statute, which is the Campaign's only basis to even be allowed access to software components that are confidential, proprietary and trade secret information and which are kept strictly sealed under Wisconsin law. Instead of seeking access for the narrow scope allowed, the Plan seeks to misuse the statute, and this Commission's authority thereunder, to further the Campaign's effort to conduct an unauthorized review based not on any concern over the accuracy of the vote tally in the November 2016

DANIEL J. FISCHER
DIRECT. 402.343.3757
DAN.FISCHER@KOLEYJESSEN.COM

elections as the statute requires but instead based on speculative, baseless, and irrational accusations of potential (not even actual) security "vulnerabilities." The Plan, and in fact the Campaign's entire request for review is the Campaign's attempt to appoint itself as the examiner of security and vulnerability of voting machines in Wisconsin, over the authority held by those federal and state agencies actually charged with testing and approving voting systems for use in Wisconsin elections.

The Vendors respectfully ask the Commission to reject the Plan, and also to reject the request for any review at this point given that the Plan reveals the Campaign's true and inappropriate intent. If the Commission should decide, however, to allow a review under the statute at this late date (more than 15 months after the election), then the Vendors ask the Commission to require the Campaign to prepare and submit an entirely new plan that actually complies with the limited scope of statute, as well as complies with the Commission's decisions on the security procedures and restrictions that will be required for any review of the software components at issue. If the Campaign is either unable or unwilling to submit a plan that so complies, then the Vendors request that the Commission deny the Campaign's request for review in its entirety.

The following is intended to highlight and discuss numerous problems with the Plan. The Vendors wish to make clear, however, that while they have endeavored to be thorough and complete, they do not waive any right, claim or defense to protect their interests, and all rights are expressly reserved.

Background

As far as the Vendors are aware, this is the first time that the Wisconsin statute has been invoked; accordingly, this is a matter of first impression for the Commission and therefore its decision is both important for the individual issues in this specific instance as well as potentially setting precedent for future requests. This is one of the necessary reasons why the Vendors seek numerous, material and meaningful protections of their confidential, proprietary, and trade secret information. The Campaign submitted a request after the November 2016 election. While the election recount has been conducted (over 15 months ago as of this letter), the original winner confirmed, and the election results certified, the Campaign has persisted in seeking a review of the software components under the guise of the statute.[1] The Commission has not yet had the opportunity to promulgate rules as to the security, review, and verification of the software components, and therefore the Vendors have made proposals in that regard and which the Commission has adopted substantially in the form proposed. However, the Vendors continue to object to the lack of any restrictions as to disclosure or publication of information obtained during a review pursuant to the statute (*see* "Non-Disclosure" section below). The Vendors also

[1] The Vendors also preserve an objection that the Campaign failed to comply with Wis. Stat. § 5.90(2) requiring a petitioner seeking a recount to establish by clear and convincing evidence that due to an irregularity, defect, or mistake committed during the voting or canvassing process the results of a recount using automatic tabulating equipment will produce incorrect recount results and that there is a substantial probability that recounting the ballots by hand or another method will produce a more correct result and change the outcome of the election. Wis. Stat. § 5.90(2)(emphasis added).

previously objected to allowing any access at the late date request, for a number of irregularities as set forth in a letter from Mike Cox on behalf of ES&S on December 9, 2016, and a letter from Ian Piper on behalf of DVS of the same date. The Vendors renew all issues and objections raised directly or indirectly by those letters. (*See* "Prior Objections" section below as well as letters enclosed herewith for ease of reference).

Throughout 2017, the Commission dealt with the unique situation created by this statute. For example, it engaged a third-party consultant (ProV&V) to assist the Commission in identifying which software components were used by the Vendors' voting systems to record and tally the votes in the November 2016 election. ProV&V, the Commission, and the Vendors worked together to identify those components with finality. The Commission also sought input from the Vendors on suggested security requirements and restrictions for any review of the software components, which the Vendors provided as referenced above.

Most recently, on January 31, 2018, the Commission held a hearing in which it received the information from ProV&V, adopted certain security measures and restrictions, and received input from its attorney as well as from the Vendors and from the Campaign. The Commission required the Campaign to submit an examination plan by February 15, giving the Vendors an opportunity to submit any objections before the Commission meets again on March 2 to discuss the next steps to take in this matter.

The Plan Fails to Comply with the Limited Scope of the Statute.

The statute reads in its entirety:

> (1) In this section, "software component" includes vote-counting source code, table structures, modules, program narratives and other human-readable computer instructions used to count votes with an electronic voting system.
>
> (2) The commission shall determine which software components of an electronic voting system it considers to be necessary to enable review and verification of the accuracy of the automatic tabulating equipment used to record and tally the votes cast with the system. The commission shall require each vendor of an electronic voting system that is approved under s. 5.91 to place those software components in escrow with the commission within 90 days of the date of approval of the system and within 10 days of the date of any subsequent change in the components. The commission shall secure and maintain those software components in strict confidence except as authorized in this section. Unless authorized under this section, the commission shall withhold access to those software components from any person who requests access under s. 19.35(1).
>
> (3) The commission shall promulgate rules to ensure the security, review and verification of software components used with each electronic voting system approved by the commission. The verification procedure shall include a determination that the

software components correspond to the instructions actually used by the system to count votes.

(4) If a valid petition for a recount is filed under s. 9.01 in an election at which an electronic voting system was used to record and tally the votes cast, each party to the recount may designate one or more persons who are authorized to receive access to the software components that were used to record and tally the votes in the election. The commission shall grant access to the software components to each designated person if, before receiving access, the person enters into a written agreement with the commission that obligates the person to exercise the highest degree of reasonable care to maintain the confidentially of all proprietary information to which the person is provided access, unless otherwise permitted in a contract entered into under sub. (5).

(5) A county or municipality may contract with the vendor of an electronic voting system to permit a greater degree of access to software components used with the system than is required under sub. (4).

Wis. Stat. § 5.905. The statute expressly limits the Campaign's review to only the "software component[s]," as defined and determined by the Commission, "used to record and tally the votes." Wis. Stat. § 5.905(1) – (4). "[S]oftware component" is only defined to include "vote-counting source code, table structures, modules, program narratives and other human-readable computer instructions used to count votes with an electronic voting system." § 5.905(1). By listing what shall be included in the defined term as only some parts of an entire "electronic voting system," the statute must be read to intend that only some parts, and not the entire voting system, are subject to review by the Campaign. Notably, the statute also directs the Commission to determine which software components are necessary to enable review and verification "of the accuracy of the automatic tabulating equipment used to record and tally the votes cast with the system." §5.905(2). By this direction, the statute makes clear that the only components subject to review are those as defined and as also determined by the Commission to "correspond to the instructions actually used by the system to count votes," that is, to review and verify the "*accuracy* of the automatic tabulating equipment." § 5.905(2) –(3).

Wisconsin law is clear that the statute must be read strictly and narrowly. When statutes create a new right not provided by the common law, "[s]uch statutes are to be construed narrowly and strictly." *Van v. Town of Manitowoc Rapids*, 150 Wis. 2d 929, 934, 442 N.W.2d 557, 559 (Ct. App. 1989)("It is a cardinal rule that where a new right has been given by statute and a specific remedy provided by statue, the right can be vindicated in no other way than that prescribed by statute.") (citing *Schaut v. Joint School Dist. No. 6*, 191 Wis. 104,m 107-08, 210 N.W. 270, 272 (1926) and *Rose v. Schantz*, 56 Wis. 2d 222, 227, 201 N.W.2d 593, 597 (1972)).

The Plan violates the statue by purporting to undertake a review that far exceeds the limited authority provided by the statute. Under Wisconsin law, the Commission must view the Plan through the lens of reading the statute narrowly and strictly when considering whether the Plan complies with the limited scope of the statute, which is to merely verify the accuracy of

recording and tallying the votes in the November 2016 election. Such review does not and cannot include looking for potential vulnerabilities or testing various hypotheses, particular without any evidence that any vulnerability exists or whether any vulnerability was exploited or otherwise affected the election in November 2016. Because the entire purpose of the Plan is to conduct inquiry into areas outside of that allowed by the statute, the Plan is void on its face and the review cannot be allowed.

The Plan also unfairly asks the Commission to exceed its own authority by permitting a review that exceeds the scope of the statute, and thereby the power to permit such review. "An administrative agency has only those powers that are expressly conferred or necessarily implied from the statutory provisions under which it operates. In determining whether an agency has exceeded its statutory authority in promulgating a rule, we examine the statute that authorizes the agency to promulgate rules." *Conway v. Bd. of Police & Fire Comm'rs of City of Madison*, 256 Wis. 2d 163, 174, 647 N.W.2d 291, 296–97 (Wis. App. 2002) (internal citations omitted). "To determine whether a rule exceeds an agency's statutory authority, we examine the enabling statute to ascertain whether the statute grants express or implied authorization for the rule. An agency's enabling statute is to be strictly construed, and we resolve any reasonable doubt pertaining to an agency's implied powers against the agency. An administrative rule that exceeds an agency's statutory authority is invalid." *Wisconsin Builders Ass'n v. Wisconsin Dep't of Transp.*, 285 Wis. 2d 472, 483, 702 N.W.2d 433, 438 (Wis. App. 2005) (internal citations omitted). *See also State ex rel. Castaneda v. Welch*, 303 Wis. 2d 570, 586–87, 735 N.W.2d 131, 139–40 (Wis. 2007)("[A]n administrative agency has only those powers as are expressly conferred or necessarily implied from the statutory provisions under which it operates." To determine whether the legislature expressly or implicitly authorized the [agency] to promulgate a rule, we first examine the enabling statute. We strictly construe an agency's enabling statute and "resolve any reasonable doubt pertaining to an agency's implied powers against the agency.") (internal citations omitted).

Here, the statute is clear as to the limited scope of the review. The courts will "strictly construe" what authority the statute gives to the Commission, which is consistent with Wisconsin law that also requires the statute itself to be narrowly and strictly construed as discussed above. Accordingly, the Plan is not just a matter of the Campaign seeking to exceed the review permitted by the statute (which it is and for which it should be denied), it is also a matter of asking the Commission to exceed its authority on the scope of review it is permitted to allow.

The Plan is Flawed.

In addition to proposing a review that far exceeds the scope and clear purpose of the statute, the Plan is flawed in its purported methodology in a number of ways, any one of which is an additional independent reason to reject the Plan.

First, the statute requires that the verification procedure must correspond to the instructions actually used by the system to count the votes. § 5-905(3). That is it. Nothing more. Just verify the accuracy of how the votes were counted. But the Plan wants to examine potential, hypothesized security vulnerabilities without any evidence that any such thing

occurred. In fact, the Plan includes in part a revolving procedure to try to invent vulnerabilities. This goes well beyond the statute as discussed above, and it also is the responsibility of the federal and state certification agencies and their corresponding testing procedures for requisite approval of voting systems before such systems can even be used in an election in Wisconsin. The statute does not allow the Campaign to propose a plan that allows the Campaign to be a self-appointed third party regulator of security and vulnerability testing. Nor would the Commission want to allow parties with ulterior motives and agendas to be able to do that. The Plan does not even seek to identify actual vulnerabilities; rather, it is looking to create them through unfounded hypotheses that have never been experienced in any election using the voting systems at issue.

Second, the Plan is flawed because it proposes to perform open ended vulnerability testing ("OEVT") analysis as developed by the national Institute of Standards and Technology ("NIST"). However, NIST was unable to persuade the Election Assistance Commission ("EAC") as to the need to incorporate such vulnerability testing into its standards for voting systems. Indeed, the "vulnerabilities" that OETV supposedly seeks to uncover have never once been known to actually occur. Furthermore, such speculative concerns over possible vulnerabilities has been rejected by courts as a basis to gain access to confidential and proprietary source code. (*See, e.g. Banfield* and Stein cases from Pennsylvania discussed below.) Indeed, the Plan's very description of OEVT testing admits a purpose well beyond the statutory limit of verifying the "accuracy" of recording and counting the votes, to wit: OEVT is intended "to facilitate the discovery of flaws in voting software architecture, design, and implementation that may not be detected by routine testing and can be exploited to change the outcome of an election." (Plan at p. 3).

More specifically, the OEVT protocol was a 2007 proposal to the EAC, which was nine years before the time of the election at issue. The EAC rejected the OEVT proposal, which the Plan admits. (Plan at p. 9). In fact, the proposal was made by a single member of the TGDC (Technical Guidelines Development Committee of NIST) and was rejected by the EAC for inclusion in the VVSG standards after approximately one year of public hearings, industry panels, and debate. The OEVT protocol received meaningful review and consideration, and the very fact that the EAC rejected it after such careful consideration is strong, credible evidence that the Plan is not viable and must not be allowed. Indeed, the Campaign seems to be proceeding on a belief that it should be allowed to do what the EAC did not find persuasive or useful 11 years ago after carefully vetting the same.

Third, the statute does not give the Campaign, or any petitioner, the right to conduct an OEVT analysis, as the statute specifically limits the review and does not give the Campaign access to sufficient components of the voting systems to conduct a security and vulnerability analysis nor does the scope of the statute allow for such analysis. The software components which "record and tally the votes" are only a part of the entire voting system. A security and vulnerability analysis, such as the OEVT protocol proposed by the Plan, would require end-to-end access to the *entire system*, and that is not permitted under the statute for at least the most obvious reason that the statute does not grant access to the entire system. The Plan's proposed OEVT review seeks to do more than just confirm the accuracy of tabulating the votes and requires more components than the Campaign is permitted to access and inspect under the

statute. The fallacy of the Plan is perhaps best summarized in this analogy: The Campaign wishes to inspect the electronic door locking mechanism, the intruder alarm, the keyless entry and ignition system, and the onboard navigation controls of a car when all the Campaign is entitled to do is confirm that the odometer is working correctly. To put this back into terms of a voting system, a true vulnerability test—like those already rigorously performed at the federal level for these voting systems—would require all of the Vendors' respective proprietary software, firmware and hardware as well as all of the commercial off-the-shelf products necessary to run each voting system. By way of examples, for ES&S that would include software modules such as Audit Manager, Election Data Manager, Hardware Programming Manager, Election Reporting Manager, ES&S Image Manager, Electionware, Election Reporting Manager, Event Log Service, Removable Media Service, AutoMark Previewer and ExpressVote Previewer, and for DVS that would include election management software modules Election Event Designer, Election Data Translator, Data Center Manager, Audio Studio, and the Election Reporting Module. Yet none of these components are identified by ProV&V and determined by the Commission as components involved in recording and tallying the votes and subject to the limited review allowed by the statute.

By way of example, the Plan proposes to "identify all input interfaces that may be subject to malicious input scenarios" yet such identification is not possible because the statute only permits access to those software components that record and tally the votes. As another example, the Plan intends to "identify inputs and internal probes that will induce errors" and "inputs and internal probes that will invoke code segments" that it believes were not "exercised" by the Vendors or the administrative agencies responsible for testing and approving the voting systems. (Plan at p. 10). Put simply, the Campaign will not have, as is not entitled to have, access to all such inputs. Furthermore, these descriptions are also evidence of the earlier point that the Plan goes well beyond the limited purpose of the statute, and that it is being attempted without any evidence that any such inputs or internal probes caused (or could cause) any issue with recording and counting the votes in the November 2016 election.

It is important to note that the Vendors do <u>not</u> make this argument to be heard, expressly or impliedly, that the Campaign should be allowed to do any type of review of, or have access to, an entire voting system. Indeed, the Vendors assert just the opposite. The Campaign is not entitled to access greater than the statute allows (which components the Commission, through its consultant ProV&V, has already determined), and the statute only allows access to certain components, and only for a limited purpose. The discussion provided here about testing a voting system from end to end is provided solely for the purpose of further demonstrating why the Plan is flawed, why it greatly exceeds the limited scope and purpose of the statute, and why it should be denied. The Vendors maintain strong objection to any suggestion or assertion that the Campaign should be allowed to conduct any type of vulnerability test and/or that it should have access to an entire voting system. Indeed, the fact that the Plan proposes a review that would require study of an entire voting system is a reason to deny the Plan and deny the requested review; it is not and cannot be a basis to allow the Campaign greater access than permitted by the statute.

Fourth, the very premise of the Plan ignores security procedures relating to the machines in addition to the security protections in the machines. For example, the Commission's regulations and Wisconsin election law put physical safeguards into place that also prevent the theoretical and speculative hacking and vulnerabilities the Campaign claims as a basis for its Plan. For example, the voting machines are secured in locked facilities, access to the voting machines is limited to specific authorized individuals, the voting machines are updated and maintained, and the voting machines are tested and accounted for through logic and accuracy before each election.

Performing the extensive security and vulnerability testing via OEVT as proposed by the Plan would require end-to-end access to the entire voting system. This is well beyond the purpose and scope of the statute, and it is not possible given the limited components to which access is permitted as recommended by ProV&V and already determined by the Commission.

Furthermore, the Commission itself has already described circumstances that both generally and specifically undermine the Campaign's ability to appoint itself an examiner and perform the review and testing it is trying to go beyond the statute to conduct, to wit:

- The Commission already subjects the voting systems to a number of steps and procedures before approval, such as review by the Commission's staff and an advisory panel of local officials before demonstrations by the vendor in a series of mock elections and then a separate demonstration for members of the public, including persons with disabilities and with Legislators. Finally, the Commission staff and the advisory panel review test results and organize yet another demonstration at a Commission meeting, which then in turn reviews and considers the evaluations made by the advisory panel and staff before making a final determination of whether to approve the voting system for use in Wisconsin elections. (http://elections.wi.gov/elections-voting/voting-equipment/approval-process, last accessed February 26, 2018).

- The Commission is required by Wis. Stat. § 7.08(6) to direct an audit of each voting system used in the state to determine the error rate of the system in counting ballots validly cast by electors. Hand-counted ballots are compared with voting system results for the same ballots. Such audit occurs following the November general election. **Notably, the Commission has explained that a piece of equipment has never failed to meet the standards established for such audits (no more than 1 error in 500,000 ballots) since the audits began in 2006.** (http://elections.wi.gov/elections-voting/voting-equipment/audit, last accessed February 26, 2018)

- The Commission has its own "voting equipment security protocols" designed to ensure the integrity of Wisconsin elections. Such protocols begin with requiring federal certification of the voting system., which is then followed by testing and certification at the state level to ensure compatibility with Wisconsin election law. The protocols also include initial logic an accuracy testing of voting system

programming, public testing of the equipment before an election, security procedures the day of an election, and post-election testing. Such pre-election testing includes verification of programming by feeding pre-marked ballots (called a test deck) through the voting systems and comparing the results with the known statistics of the test deck. Indeed, the test decks used for the public test of the voting systems is different than the test decks used during the programmer testing of the voting systems, "so that errors in programming do not remain undetected." Also, "an errorless count is required at the conclusion of the process and any anomalies identified in this testing must be remedied before the equipment can be approved by the clerk for use in the election." Once the voting systems pass pre-election testing, they are secured and a chain-of-custody log is maintained to document any access or transfer of each memory device. Such procedures are specifically designed "to protect against malicious breaches to electronic voting equipment components as well as provide transparency of justifiable access." Such security procedures include the use of tamper-evident seals with unique serial numbers, which are verified again individually before the polls open on election day and again after the polls close. (http://elections.wi.gov/elections-voting/voting-equipment/security, last accessed February 26, 2018).

- The Commission's Chairperson was quoted by Channel3000.com (Wisc-TV News 3, Madison) shortly after the election as stating the Stein Campaign recount revealed no evidence of any hacking, despite the Campaign's allegations in Wisconsin, Pennsylvania, and Michigan. "It is my understanding that we found no evidence of any hack in terms of our computer infrastructure system." (*Trump Adds 131 Votes in Wisconsin Recount*, by Jessica Arp, December 12, 2016; https://www.channel3000.com/news/politics/trump-adds-131-votes-in-final-recount-tally/207438787, last accessed February 26, 2018).

The Alleged Security Vulnerabilities Are Speculative and Theoretical Only, and They are No Basis to Approve the Plan

As discussed throughout these objections, the Plan claims to test for purported security vulnerabilities rather than the accuracy of recording and counting the votes in the November 2016 election. As such, the Campaign is seeking to supplant the EAC, supplant independent and authorized third-party voting system test laboratories ("VTSLs")—which are charged with specific security and vulnerability testing—and supplant this Commission's state-level testing of voting systems. The statute does not allow the Campaign to do so. The voting systems already undergo significant testing in advance of approval for use in a Wisconsin election. By way of summary example, at the federal level, the EAC receives and reviews testing reports from VTSLs which test the voting systems against Voluntary Voting System Guidelines ("VVSG") standards established by the EAC. The VVSG are a set of specifications and requirements against which voting systems are tested to determine if the system meets all required standards and will be approved by the EAC. The Help America Vote Act ("HAVA") mandates that the EAC develop and maintain these specifications and requirements. In addition to developing and

maintaining the standards, the EAC also actively monitors the testing throughout each step, which occurs only after the EAC approves the initial voting system application and corresponding lab test plan. The EAC also reviews and approves the final lab test reports issued by the VSTLs. Such testing includes:

- Source code review for conformance with established, published standards;
- Technical data package review, wherein all technical documentation is studied for completeness and accuracy, and which is then later used to ensure thorough testing of all system functions;
- Compliance builds, meaning the reviewed source code is compiled for use in all subsequent tests;
- System set-up, wherein all components are assembled and loaded with firmware, operating systems, and compiled software as specified;
- Hardware testing (both environmental and electrical);
- Volume and stress testing, in which the system is put under substantial workloads;
- System integration testing;
- Security testing, which includes testing the physical system, the operating system, and the software and firmware;
- Usability testing, such as from the perspective of a voter and a poll worker;
- Accessibility testing, such as from the perspective of a person with a disability;
- Data accuracy testing;
- Regression testing, wherein any bug fixes developed during testing are tested again to confirm the fix and ensure no other system functionality was affected by the change;
- Physical configuration audit; and
- Function configuration audit.

At the state level in Wisconsin, testing includes:

- Logic and Accuracy testing for Wisconsin-specific elections, and that includes such steps as

- General partisan election, no Straight Part, with special nonpartisan election sections;
- Open primary with party preference, which is a unique primary election used in Wisconsin; and
- Presidential primary election, which is an election test that follows standard open primary logic;

- Modem Field testing, which tests the ability of the system to modem unofficial election results using 2-3 Wisconsin counties' existing infrastructure; and
- Documentation review.

The state level testing is an extensive end-to-end functional test and a thorough assessment of compliance. In addition to these procedures, voting machines are loaded and tested before each election, following specific logic an accuracy testing protocols, tamper resistant seals are installed on the machines, and the machines are kept under secure, locked, access-controlled storage. Notably, at the federal level, the rigorous EAC testing procedures have separate defined steps and processes for security testing and for data accuracy testing. That is instructive here, as the statute only allows the Campaign to verify the accuracy of recording and tallying the votes, not conduct security and vulnerability testing as proposed in the Plan.

The Campaign Has Already Been Denied This Type of Testing

The Campaign tried to force the same type of security and vulnerability testing in Pennsylvania, asking for a recount by claiming—without evidence—that the electronic voting systems in the state (DRE machines as well as optical scanners like those used in Wisconsin) might have been "hacked." The Pennsylvania federal court quickly denied and dismissed the campaign's attempts, stating "[m]ost importantly, there is no credible evidence that any 'hack' occurred, and compelling evidence that Pennsylvania's voting system was not in any way compromised." *Jill Stein v. Pedro A Cortes*, 2:16-cv-6287-PD, Filing No. 1 at p. 1 (E.D. Pa. December 12, 2016). In discussing the many reasons to dismiss the Campaign's claims, the Court noted that the Campaign had organized supporters in some districts to request a recount because the petitioners purportedly had "grave concerns about the integrity of the electronic voting machines used in their districts," yet the Campaign and the supporters failed to provide the necessary affidavits for such a challenge, nor did they provide even one allegation that any hacking had actually occurred. (*Id.* at p. 5). Those supporters dropped their claim rather than post the bond required to do the recount. *Id.* The court also discussed other, similar Campaign efforts throughout the state, and noted that no state court had ordered any forensic review of the electronic voting machines that the Campaign sought, and two courts had specifically rejected such requests. *Id.* at p. 6. The federal court quoted one such state court judge as ruling, "Pennsylvania law simply does not mandate or allow a candidate to perform a forensic examination of the DRE electronic voting system, and she [the state court judge] would not impose requirements the Legislature has not seen fit to establish, particularly where there is

absolutely no evidence of any voting irregularities." *Id.* at 7 (quoting *Stein v. Phila. Cty. Bd. of Elections*, No. 161103335 (Pa. C.P. Ct. Phila. Cty. Dec. 7, 2016)(internal quotations omitted).

Similar to what the Campaign is trying to do in Wisconsin now with its proposed Plan, the Campaign argued in Pennsylvania that notwithstanding the certifications of the voting machines, the Campaign believed "possible vulnerabilities have abrogated their right to vote." *Id.* at p. 9. The federal court rejected this concern and its basis entirely. In doing so, the court cited to a similar effort by the Campaign in Michigan, wherein the Michigan judge found: "Plaintiffs have not presented evidence of tampering or mistake. Instead, they present speculative claims going to the vulnerability of the voting machinery—but not actual injury. Because mere potentiality does not amount to a claim that the vote was not fairly conducted, Plaintiffs' new claims are insufficient to maintain the existing TRO [which was struck down on appeal because Stein was not an aggrieved party under Michigan law]." *Id.* at p. 10 (quoting *Stein v. Thomas*, No. 16-14233, Doc. No. 36 at p. 7 (E.D. Mich. Dec. 7, 2016)). In the Pennsylvania federal court case, the court noted that Plaintiffs claimed the voting machines were "vulnerable, hackable, [and] antiquated" and that neither Dr. Stein nor her voters have been permitted to examine them, but then it found that such speculative and unsubstantiated concern failed to even meet the threshold for standing to ask for the relief they sought. *Id.* at. p. 13-15. "In sum, because Plaintiffs have alleged speculative injuries that are not personal to them and could not be redressed by the relief they seek (or any relief I could order), they are without standing to bring their claims. *Id.* at p. 15. The court also noted that the Plaintiffs' expert evidence was no more than the allegations: the "theoretical possibility that Pennsylvania's voting machines may have been hacked," and such evidence was insufficient to justify taking any action the Campaign requested. *Id.* at 16.

The federal court concluded its order by explaining how the Campaign's alleged concerns over hacking and potential vulnerabilities was simply not credible, and also that the state's expert was highly credible that no such vulnerabilities exist. *Id.* at 25-30. "Plaintiffs have presented no credible evidence, however, that any such tampering occurred or could occur; the Commonwealth presented compelling evidence that it did not." *Id.* at 25. "While the state's expert acknowledged the theoretical possibility that an individual DRE machine could be hacked, he credibly explained that in light of all of the protections in place, the suggestion of widespread hacking borders on the irrational." *Id.* at 28 (emphasis added). "[A]s I have found, suspicions of a 'hacked' Pennsylvania election borders on the irrational." *Id.* at 31. A copy of the Pennsylvania federal court order is enclosed for reference.

Furthermore, the *Banfield* case, which was cited by the Pennsylvania federal court, is yet another example of the irrational and baseless allegation of potential hacking or vulnerabilities of electronic voting machines. In *Banfield*, the petitioners argued that Pennsylvania's DRE voting machines should not be used because they had alleged security vulnerabilities that lead to insufficient protection against tampering. Banfield rejected the petitioners' claims because the claims advocated for the voting machines be held to an impossible standard of invulnerability. The court agreed with the state that the mere possibility of error cannot be the basis to reject a voting system because any voting system—even hand counting—is subject to the "unfortunate reality" that error of some kind is possible and cannot be completely eliminated. *Banfield v.*

Cortes, 631 Pa. 229, 260, 110 A.3d 155, 174 (2015). *Banfield* concluded that determining the adequacy of security measures against tampering necessarily results in a subjective determination which the Legislature delegated to the Secretary of the Commonwealth. *Banfield*, 631 Pa. at 260-61, 110 A.3d at 174. Accordingly, the petitioners' claims failed on summary judgment because they "had not shown any more than the mere possibility that the certified DREs in theory could be subject to tampering, presenting no evidence that the challenged devices have failed to accurately record votes or experience a security breach in an actual election." *Banfield*, 631 Pa. at 261-62, 110 A.3d at 174-75

The Commission should consider the Pennsylvania cases as part of its decision to reject the Plan because the cases further evidence that (a) the Campaign has unsuccessfully tried to make its security and vulnerabilities allegations before and in other places; (b) the speculation and theoretical hypothesizing that vulnerabilities possible could exist has been thoroughly reviewed and rejected by other authorities as an insufficient basis to examine the voting machines; and (c) the Campaign's true motive here is not to comply with the limited scope of the Wisconsin statute but rather to attempt to misuse the statutory purpose for access to take a second bite (or perhaps more accurately a fourth or fifth bite) of the proverbial apple, that is, to search for vulnerabilities that it has no evidence exist or have affected any election.

The Plan's Timeline is Far Too Long and is Further Evidence that It Seeks to Do More Than Allowed:

The Plan seeks to start a 90+ day schedule on March 5. The Plan begins its time line too soon, and it proposes far too long for its review. It also purports to reserve time to be revised later, which is unacceptable. Approval of such a provision allows the Plan to subvert the very reasons the Commission had for directing the Campaign to submit the Plan by a date certain in the first place. The Vendors and the Commission need time to review what the Campaign intends to do in the examination room, so that improper and unauthorized activities like those proposed in the Plan now, can be addressed before the Campaign is ever given access to the Vendors' confidential, proprietary, and trade secret information. The Campaign should be required to submit a definitive and fixed final plan for the narrow scope of review allowed. Such work should not exceed one or two business days. The Plan should not be allowed to state that the Campaign intends to adjust the Plan and its activities during the examination. And while the Plan suggests and proposes a 90-day time frame, it surreptitiously includes a longer time frame when it proposes that it will continue developing and testing hypotheses "until the set of hypotheses or the examination resources are exhausted." Apparently, the Campaign believes it can continue to study the components and find ways to induce errors or cause problems (that have never been experienced) for as long as it can continue to think up new ways to do so or it runs out of money to keep paying the examiners to do so. This goes boldly and wildly beyond the limited purpose and scope of the examination allowed by the statute. The statute simply allows a candidate who has requested a recount to also confirm that the votes counted by electronic voting machines was done accurately.

The very fact that the Plan purports to be as "involved" as it is and that it suggests it needs at least as much time as it proposes is further evidence that the Campaign intends to act well beyond the limited purpose of the statute. Security and vulnerability matters involve a longer and more in depth review, but such review is beyond the scope of the statute and therefore beyond the rights of the Campaign to conduct.

The Plan Does Not Follow Restrictions Already Directed by the Commission

The statute requires the Commission to promulgate rules to ensure security when a review is approved by the Commission. Furthermore, no review is allowed unless each individual involved in the review first agrees in writing to the restrictions and security procedures put in place by the Commission. Pursuant to this directive, the Commission adopted several security protocols and restrictions. These were some, but not all, of the protocols proposed by the Vendors, and the Vendors reserve their rights to object regarding any proposed protocol not adopted by the Commission. (*See, e.g.*, section on "Non-Disclosure" below). The Campaign has been aware of the Commission's protocols while it developed the Plan, so it has no excuse for the Plan exceeding those protocols. By way of example and not limitation, the Plan states that it intends to bring computer equipment pre-installed with software as well as other equipment into the room, but such outside computers and equipment are not allowed. In another example, the Plan proposes to bring and install software it describes as "bug finding" into the examination, which is also beyond the scope of the review and contrary to the protocols established by the Commission. Still further, the Plan proposes to test a "broader set of software components" later in the schedule, but it is only permitted to inspect the identified software components as set forth in the statute and determined by the Commission.

The Plan Has too Many Staff Unless Its Intent is to Exceed the Statute's Limited Scope

The statute allows the Campaign to designate "one or more persons" who are authorized to receive access to the software components, but in light of the limited purpose and scope of the statute, a team of 16 or more persons who work 145+ "person-weeks" trying to find or induce flaws in the software is patently unreasonable. (Plan at p 11). The purpose of the review is limited, and so too should be the corresponding work and personnel utilized to conduct the review. Furthermore, the Plan proposes to advise the Commission only one week in advance of who will be coming on site to access the Vendors' highly confidential, proprietary materials. The Vendors need more notice as to the individuals so that they can adequately investigate each of them and determine whether there is an objection to their participation in the review, and the Commission needs an opportunity to make a determination on such matters. There must be sufficient time to run proper background checks on each individual proposed, and such costs should be paid by the Campaign as the one proposing to allow each such individual access to the Vendors' confidential, proprietary, and trade secret information. One week is not enough time for such work, particularly as the Plan suggests the various teams may change for each review it proposes.

Perhaps ironically, the Plan's purported testing for security vulnerabilities is threatened by the very staffing it proposes to do such work. One of the many reasons why the Vendors

work diligently to limit access to their voting software and any component thereof is the simple and undeniable proposition that the more people who are given access to such materials, the greater the chance/risk for an accidental, reckless, or intentional disclosure. The Vendors also hope the Commission will consider the practical perspective gained from now having the Plan and seeing what the Campaign wants to do. The Campaign has an agenda. This agenda has been rejected, repeatedly, in other states, but the Campaign now wishes to push its agenda in Wisconsin by exceeding the scope of the statute. The people working for the Campaign in this endeavor are likely to be those who continue to perpetrate the speculation and baseless claims against electronic voting machines and purported "vulnerabilities." These are the very people who should not be given direct access to confidential, proprietary, and trade secret software. Yet, the Plan suggests the Campaign will provide merely a name and corresponding "qualifications" a week in advance (Plan at p. 11), which does not allow the Vendors or the Commission sufficient time or information to properly investigate and vet the proposed individuals before they are given access to the Vendor's confidential, proprietary, and trade secret materials.

Non-Disclosure is Necessary and Must be Mandatory as a Condition of Access

The Plan acknowledges that any staff member who is given access to the software components should do so "only upon execution of the Confidential Non-Disclosure Agreement provided to the individual by the Commission." Previously, the Commission considered the necessary restrictions requested by the Vendors that those who are given access to the Vendor's confidential and proprietary information must be prohibited from disclosing or publishing what they learn. The Commission has not adopted that restriction, and the Vendors object to proceeding without such a restriction.

If a court were to allow an expert access to such software components in the context of a lawsuit, the expert would not be allowed to publish or talk about what he or she learned, nor would he or she be allowed to use anything learned outside of the litigation itself. This is a routine limitation imposed by state and federal courts across the country, pursuant to procedural rules that allow them to do so. See, e.g. Fed. R. Civ. P. 26(c)(1)(G) (permitting orders requiring that trade secret or other confidential information not be revealed or revealed only in specified ways). Yet here there is a suggestion that anyone allowed access to the Vendor's confidential, proprietary, and trade secret information should be given similar access and not be so limited, despite the Plan's very acknowledgement that each staff member should sign an agreement as to "confidentiality" and "non-disclosure." There must be, as part of the security requirements and restrictions imposed by the Commission, a requirement of absolute confidentiality and non-disclosure of the information obtained, and also a restriction that the information is used solely for the limited purpose that access is granted, that is, to verify accuracy in recording and counting the votes. No right of free speech is threatened by this, as no one has a free speech right to divulge the trade secrets of another. Furthermore, the language of the statute itself necessitates the restriction requested by the Vendors. The statute requires the Commission to "secure and maintain" the software components "in strict confidence," and that the Commission withhold disclosure from public records requests, and further that the Commission impose compliance with the "highest degree of reasonable care" to maintain the confidentiality of all

proprietary information. This necessarily means that anyone who is given access to the software pursuant to the statute must be prohibited from publically disclosing or discussing what they reviewed, particularly when the statute is to be read narrowly and strictly as to the right it creates. If any review is to be allowed—which of course would first require the Campaign to submit a new plan that does not exceed the scope of the statute—then the non-disclosure agreement that each person must sign must include the Vendors' restriction on publication and speech.

Such a restriction also makes sense in light of the Campaign's purported concern over alleged security and vulnerability issues. If the security of election results is paramount, then publically discussing or publishing any identified vulnerability (assumed here only for the purpose of argument, as such threats have only been speculative and never experienced in reality) only increases the threat to elections. Any such information should be shared with the Vendors and the Commission only so that any such issue could be considered and corrected. Discussing it publically only provides information to those who might try to exploit it. (Again, this argument assumes a vulnerability only for a discussion of the illogic of disclosing the vulnerability publically and does not admit that any such vulnerability exists, has existed, or has ever been experienced in any election.)

Prior Objections

Both ES&S and DVS submitted letters in opposition to the Campaign's request for review of the software components. The letters were each dated December 9, 2016, and are enclosed herewith. The Vendors renew their objections as raised by the letters. It was clear to the Vendors in December 2016 that the Campaign had a motive and an agenda for the requested review that did not go to the recount in Wisconsin nor did it relate to confirming the accuracy of recording and tallying the votes. Indeed, the Campaign attempted the same thing, arguing the same speculative "vulnerabilities" in Pennsylvania and Michigan, and it was rejected at every instance. The Plan now submitted by the Campaign in this matter proves the Vendors' suspicious that this is but another attempt at the same thing. It is old wine in a new bottle. It was not allowed in Pennsylvania and Michigan, and it should not be allowed here.

Conclusion

The Plan expressly states: "We all share the overarching goal of ensuring that Wisconsin elections are *secure*." (Plan at p. 3) (emphasis added). The problem is, the Campaign is not permitted to verify security, only accuracy. The Plan is and has been flawed from inception and must be rejected as a failure to comply with the limited scope and purpose of the statute. The Campaign did not challenge the election results, and it has not alleged any tampering nor offered any evidence of actual tampering. The Campaign must not be allowed to now proceed with an examination plan that purports to test for vulnerabilities of entire voting systems in this context and within the limited confines of verifying the accuracy of those specific software components that record and tally the votes. The Campaign is following its own agenda and is not seeking to serve any public good for the security of elections. Federal and state agencies, as well as authorized independent testing laboratories, are charged with security and vulnerability matters.

Furthermore, the November 2016 election votes were recounted and the results certified long ago. As recognized by agencies such as the Department of Homeland Security, voting systems have become seen as "critical infrastructure" in our society, and allowing the Campaign to exceed the scope of the statute and of the Commission's authority to try to haphazardly jeopardize that infrastructure cannot be countenanced. The Vendors respectfully ask the Commission not to allow the Campaign to proceed with the Plan.

We thank the Commission for this opportunity to provide input, and we stand ready to answer any questions the Commission may have or if there is anything its members would like to discuss.

Very truly yours,

Daniel J. Fischer

DJF/tlc

Attachments

KOLEY JESSEN

ATTORNEYS

KOLEY JESSEN PC, LLO
1125 SOUTH 103RD STREET
SUITE 800
OMAHA, NE 68124
PHONE. 402.390.9500
FAX. 402.390.9005
koleyjessen.com

December 9, 2016

VIA EMAIL TRANSMISSION
michael.haas@wi.gov

Michael Haas, Administrator
Wisconsin Elections Commission
212 East Washington Avenue, 3rd Floor
P.O. Box 7984
Madison, WI 53707-7984

Re: Election Systems & Software, LLC - - Stein Access Request
Our File No. 01928-0256

Dear Mr. Haas:

We represent Election Systems & Software, LLC ("ES&S") and it has requested that I respond to your letter of November 7, 2016, relating to the request from Jill Stein for access to certain "software components" of ES&S voting equipment used in Wisconsin during the November 2016 Presidential Election. We have several concerns about the request. You recognize some of them in your letter in that the statutory provision under which the request is made has not been invoked in Wisconsin since the legislation was enacted in 2005 and there are uncertainties surrounding its implementation when read in the context of the entire statutory scheme of which it is a part.

Under Wis. Stat. § 5.905(1) the term "software component" is defined as vote counting source code, table structures, modules, program narratives and other human - readable computer instructions used to count votes with an electronic voting system. Subsection 2 of that statute requires the commission to determine which software components of an electronic voting system it considers to be necessary to enable review and verification of the accuracy of the automatic tabulating equipment used to record and tally votes cast with the system. It goes on to state that the commission shall require each vendor to place those identified software components in escrow with the commission within a certain timeframe. The commission then has to secure and maintain those software components in strict confidence except as authorized in this section.

To our knowledge, none of that has never been done. ES&S has no record of the commission identifying the specific software components necessary to enable the subject review

MICHAEL C. COX
DIRECT. 402.343.3703
MIKE.COX@KOLEYJESSEN.COM

nor have any such specific software components been put in a separate escrow with the commission. While there are certainly materials in escrow relating to ES&S' entire voting system, those would include all components relating to its voting system - - not just "software components" to be identified necessary to enable review and verification of the tabulating equipment used to tally the votes - - although they are certainly included in these materials.

Moreover, subsection 3 of the statute requires the commission to promulgate rules to ensure the security, review and verification of the software components used with each electronic voting system. We have not found, nor could you point us to, any rules promulgated under subsection 3.

ES&S calls attention to these matters because under paragraph 4, access is only to be granted by the commission to "software components" that have previously been specifically identified and placed in escrow with the commission. Further, other than a broad reference to a written agreement that obligates the recipient to exercise the "highest degree of reasonable care to maintain the confidentiality of all proprietary information to which the person is provided access" there are no other security, review or verification parameters described and no rules relating to the same have been promulgated under subsection 3 as required.

Moreover, access is only to be granted if a valid petition for a recount has been filed. Wis. Stat. 5.905(4). While most likely a moot point at this juncture, ES&S does not believe a valid petition for a recall was filed under § 9.01 as the specifics required in the petition were not met. Notwithstanding the foregoing, the recount has commenced and indeed is almost complete and we are advised that there is no material change with respect to a vote count or who is the winning candidate. That would be particularly true as to the party to this recount, Jill Stein, who received a very small percentage of the votes in Wisconsin. She has publicly stated that she does not expect the vote count to change but instead has also publicly stated that she wants (and has asked for both in Pennsylvania and Wisconsin if not also Michigan) what amounts to a referendum on electronic voting. ES&S does not believe that such is the subject of a valid petition for a recount, nor can the applicable statute be utilized for the same. There must be some good faith threshold attached to the access request and there is no evidence that such exists at this point in time given the delay in requesting such access, the fact that the Wisconsin recount will be completed by Monday and the fact it does not appear that under any circumstances that the vote count is going to materially change from what was reported on Election Day.

Further, regarding the voting machines, there are protocols built into Wisconsin recount procedures to effectively look at individual electronic voting machines if an anomaly is detected. Presumably, candidate Stein has had the opportunity to have representatives at both pre-election and post-election testing done with the machines relating to the election and also, to the extent there has been an anomaly in a voting machine, (but ES&S is not aware of any) the ability to observe any action with respect to the same. Accordingly, it is then difficult for ES&S to understand the broad request that has been made, under a statute that has never been implemented or action taken thereunder by the commission, to review ES&S' confidential, trade secret and proprietary information at this juncture and under the current facts as they stand. Such a broad request was denied in Pennsylvania based upon some of the factors referenced above.

Michigan has ceased its recount based on the fact that Stein was not an "aggrieved candidate" under their statutes, so to ES&S' knowledge no such review is being conducted there.

Accordingly, ES&S has serious questions as to when such a request would become moot or available, given the fact there is not going to be any material change in the vote count from what was reported on Election Day; ES&S is informed that Secretary Clinton would have had to overturn all three states in order to win the Electoral College and Michigan has stopped its recount and therefore those Electoral College votes will go to Trump making any further recount in either Pennsylvania or Wisconsin a moot point as to who is the winner; and the fact that candidate Stein herself has said that she does not expect anything to change with the count and has focused now on the sole topic of the electronic voting and the feasibility of any hacking that may have occurred. In that regard, it is important to note in her petition that none of the items she claims happened around the country occurred in Wisconsin. Moreover, her "bootstrap argument" regarding absentee ballots is speculation at best and again cannot serve as a basis for ES&S to have to disclose its confidential, trade secret and proprietary information under a statute that is solely focused on a valid recount which appears no longer to exist. Such access requests cannot be made in a vacuum and it appears to ES&S that this is what is being done at this juncture.

To the extent access is granted and in response to some of the specific questions raised in your letter, it is ES&S' position that the only software components to which access need be granted are those used to record and tally the votes cast on ES&S' electronic voting system. This is limited to the firmware resident on the following ES&S precinct and central count tabulators: ES&S Optech Eagle, ES&S iVotronic, ES&S M100, ES&S DS200 and the ES&S DS850. ES&S does not believe any other "software components" would need to be reviewed. ES&S would insist that it be involved in obtaining that information from escrow to the extent access is to be provided. Those items are contained in the current escrow in the State of Wisconsin with Escrow Tech. ES&S would also insist that it be involved in transporting its firmware to the identified secure location.

With regard to any access to the firmware described above, it is important to understand that this is not a lawsuit. Therefore, the request by Stein's attorney for a "rolling production" - - a term commonly used in responding to document requests in litigation - - simply does not come into play in this matter. ES&S would insist that a separate secured room be set up where the commission is located and any person desiring to review its firmware would have to travel to that room and only upon the signing of a strict Confidentiality and Nondisclosure Agreement would access be granted. The firmware would be reviewed in a read only format on a computer terminal with no ties to the Internet or other terminals. No electronic devices of any sort including, without limitations, cell phone, usb sticks or other such devices could be attached to the terminal. No copies of any kind could be made. These are a few basic protocols that have been used in other disclosures and are not foreign to most of the people listed to whom Stein's request access be granted. Given the lack of rule promulgation with respect to security, review and verification under the subject statute, ES&S believes that these protocols are absolutely necessary to protect its confidential, proprietary and trade secret information which the same statutory sections recognize and also recognize the need for security with respect thereto.

ES&S is in the process of preparing a Confidentiality and Nondisclosure Agreement and will send that to you under separate cover letter.

Upon your review of the foregoing, please contact us to discuss the same.

Very truly yours,

Michael C. Cox

MCC/pjs

DOMINION VOTING

1201 18th St., Suite 210 Denver, CO 80202

December 9, 2016

Michael Haas, Administrator
Wisconsin Elections Commission
212 E. St Washington Ave., 3rd Floor
Madison, WI 53707

Dear Mr. Haas,

This letter is in reply to your letter of December 7th regarding the current recount in the State of Wisconsin and the release of software components used to record and tally the votes cast pursuant to Wis. Stat. s. 5.905(4). While Dominion does not have a general objection to a release at this time, Dominion respectfully reserves the right to object to the release of software components from escrow at a later date for the following reasons:

a. Pursuant to Section 5.905(2), the Commission has not determined "which software components of an electronic voting system it considers to be necessary to enable review and verification of the accuracy of the automatic tabulating equipment used to record and tally the votes cast with the system." Dominion has provided a list of software components used to record and tally the votes cast in answer to question 1 below, but the Commission has not made its determination.

b. Pursuant to Section 5.905(3), the Commission has not "promulgate rules to ensure the security, review and verification of software components used with each electronic voting system approved by the commission," and therefore Dominion is unable to determine whether or not to object in the absence of procedures.

c. If the State completes the recount prior to the escrow release of software components, any review would be moot, unnecessary and not part of a defined release condition.

d. Dominion may question the validity of the recount pursuant to Section 9.01, as there is no evidence that "a mistake or fraud has been committed in a specified ward or municipality in the counting and return of the votes cast for the office .... or that another specified defect, irregularity, or illegality occurred in the conduct of the election."

Below are Dominion's responses to the five items/questions outlined in your letter:

1. **Identify the software components used to record and tally the votes cast on electronic voting systems which Dominion has provided to Wisconsin municipalities, as described in Wis. Stat. s. 5.905**

   The following software components of the Dominion systems are used to record and tally votes cast in the State of Wisconsin:

1.1 ImageCast Central 4.14.17

\ICC_4-14-17_SourceCode_TechDocs.zip\Source Code\ICC_Source

Below is a listing of the relevant files.

Folder	Files
cf2xx	DvsTotalResults.*
cf2xx	Tabulate.*
cf2xx	TabStructure.cpp
election	*.*
core	DvsSecure*.*
common	DvsFile.*
common	DvsUtils.*

1.2 ImageCast Precinct 4.14.17

Use the WinRAR utility to extract source code files from the following compressed file:
\ICP 4-14-17\ICP_4-14-17_SourceCode_TechDocs.zip\Source Code\ICP_4.14.17-US_Source_Code\dvs.tgz

Below is a listing of the relevant files.

Folder	Files
dvs\cf2xx	DvsTotalResults.*
dvs\cf2xx	Tabulate.*
dvs\cf2xx	TabStructure.cpp
dvs\election	*.*
dvs\core	DvsSecure*.*
dvs\common	DvsFile.*
dvs\common	DvsUtils.*

1.3 ImageCast Evolution 4.14.21

Use the WinRAR utility to extract the source code files from the following compressed file:
\ICE 4-14-21\ICE_4-14-21_SourceCode_TechDocs.zip\Source Code\ICE_4-14-21_Source_Code\VotingMachine-4.14.21.tar.bz2

Below is a listing of the relevant files.

Folder	Files
VotingMachine-4.14.21\TabulatorGDomain\code\VoteRules	*.*
VotingMachine-4.14.21\BusinessServices\BusinessServicesImp\code\ResultsHandler	*.*

1.4 AccuVote-TSX BallotStation 4.6.4D

\GEMS 1-18-24D\AV-TSX\BallotStation 4-6-4D\

Below is a listing of the relevant files.

Folder	Files
Source Code	*.*

1.5 AccuVote-OS PC 1.96.6

\GEMS 1-18-24D\AV-OS PC 1-96-6

Below is a listing of the relevant files.

Folder	Files
Source Code	*.*

1.6 Insight APX 2.10

\WI 2006-10-31 Escrow Deposit – Recount\Optech Insight\

Below is a listing of the relevant files.

Folder	Files
Source Code	*.*

1.7 Edge 5.0.24

\WI 2006-10-31 Escrow Deposit - Recount\AVC Edge\AVC Edge Firmware Version 5.0.24 Source Code\CD - Source Code.zip\CD - Source Code\

Below is a listing of the relevant files.

Folder	Files
Edge 5.0 Source Code	*.*

2. **Are all of those software components deposited into escrow as required by Wis. Stat. s. 5.905(2)?**

   Yes

3. **Can the Wisconsin Elections Commission obtain and provide access to the software components directly from the escrow agent?**

   Subject to a possible objection by Dominion as stated in the opening paragraph of this letter, the Wisconsin State Elections Board ("State") is the Beneficiary to the escrow account with EscrowTech and the State can submit a request directly to EscrowTech for a copy of the escrow materials, but only for the purposes stated in the release conditions of the escrow agreement.

4. **What is the position of Dominion regarding the logistics, timing, and type of access that should be provided to the individuals identified in the request?**

   Dominion has provided source code for review in other States as part of third party subpoenas. In all cases, Protective Orders were granted to protect the security and

confidentiality of the Dominion intellectual property. Dominion requests that the State take the following logistical, security and confidentiality measures as part of the review.

4.1 The review will be undertaken at a secure, restricted access location and on reasonable notice to Dominion representation.

4.2 The source code must at all times remain within the custody, control and oversight of the State of Wisconsin.

4.3 All viewing and analysis of the source code will take place in a secure, video monitored and access controlled room and on a secure computer with tamper evident seals on all ports.

4.4 Only persons authorized by State of Wisconsin will be allowed in the room for reviewing.

4.5 Cameras, cell phones, smart phones, laptops or other computers devices, USB memory devices or any other removable or wireless media, photographic and recording devices are prohibited in the review room.

4.6 The secured computer used for review cannot be connected to any internal or external network and all software components will be fully purged and deleted from the computer or workstation at the conclusion of the review.

4.7 Information obtained during the release or viewing of the source code will be considered part of the source code and will be used by the State of Wisconsin solely for the purposes of the review and neither the State nor the reviewers will use the information for any other purpose whatsoever.

4.8 All individuals permitted to review source code must sign written confidentiality agreements prohibiting them from copying or disclosing the content of such source code.

5. What provisions do you believe are necessary to include in an agreement to maintain the confidentiality of proprietary information to which the designated individuals may be provided access?

Dominion will provide a confidentiality agreement to the State by 5:00 p.m. Central time on Monday, December 12th.

Please feel free to contact me for further questions regarding the recount procedures.

Regards,

Ian Piper
Director, Federal Certification
Dominion Voting Systems, Inc.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

JILL STEIN, et al.,	:	
Plaintiffs,	:	
v.	:	**Civ. No. 16-6287**
	:	
PEDRO A. CORTÉS,	:	
***in his official capacity as Secretary of the Commonwealth of Pennsylvania*, et al.,**	:	
Defendants.	:	
	:	

Diamond, J. **December 12, 2016**

MEMORANDUM

Unsuccessful Green Party Candidate Jill Stein and Pennsylvania voter Randall Reitz allege that because Pennsylvania's voting machines might have been "hacked" during last month's election, I must order the Commonwealth to conduct a recount of the votes cast for President. There are at least six separate grounds requiring me to deny Plaintiffs' Motion. Most importantly, there is no credible evidence that any "hack" occurred, and compelling evidence that Pennsylvania's voting system was not in any way compromised. Moreover, Plaintiffs' lack of standing, the likely absence of federal jurisdiction, and Plaintiffs' unexplained, highly prejudicial delay in seeking a recount are all fatal to their claims for immediate relief. Further, Plaintiffs have not met any of the requirements for the issuance of a mandatory emergency injunction. Finally, granting the relief Plaintiffs seek would make it impossible for the Commonwealth to certify its Presidential Electors by December 13 (as required by federal law), thus inexcusably disenfranchising some six million Pennsylvania voters. For all these reasons, I am compelled to refuse Plaintiffs' request for injunctive relief.

I. Background

On November 8, 2016, the United States conducted its Presidential Election. The reported vote shows that Republican Candidate Donald J. Trump was elected President. See Donald Trump Elected President of the United States, Associated Press (Nov. 9, 2016, 2:29 a.m.), http://elections.ap.org/content/donald-trump-elected-president-united-states-0. Although Pennsylvania has not yet certified its results, the reported popular vote indicates the following: Mr. Trump (2,970,764 votes); Secretary Hillary Clinton (2,926,457 votes); Governor Gary Johnson (146,709 votes); Dr. Stein (49,947 votes); and Mr. Darrell Castle (21,569 votes). See Unofficial Returns, Pa. Dep't of State, http://www.electionreturns.pa.gov (last visited Dec. 12, 2016). Pennsylvania has not yet certified its election results. (See Hr'g Tr. 90:1-9, 121:20-22.)

Pennsylvania has opted into the federal "safe harbor" that allows it to determine conclusively its Presidential Electors through state procedures. See 3 U.S.C. § 5; 25 P.S. § 3192. The safe harbor requires Pennsylvania to make a final determination of its Electors at least six days before the Electoral College meets. See 3 U.S.C. § 5. The Electoral College will meet on Monday, December 19, 2016. See id. § 7. Pennsylvania thus must certify its election results tomorrow to retain its right to make the final determination of its Electors. See Bush v. Gore, 531 U.S. 98, 111 (2000) (per curiam).

Some three weeks after Election Day, Dr. Stein initiated efforts to seek a recount of votes cast for President in Pennsylvania, Michigan, and Wisconsin, the three states in which Mr. Trump prevailed by the narrowest margins. E.g., Stein v. Thomas, No. 16-14233 (E.D. Mich. 2016); Great Am. PAC v. Wis. Election Comm'n, No. 16-795 (W.D. Wis. 2016); In re The Matter of the 2016 Presidential Election, No. 569 MD 2016 (Pa. Commw. Ct. 2016); Stein v. Phila. Cty. Bd. of Elections, No. 161103335 (Pa. C.P. Phila. Cty. 2016); see Recount2016,

Jill2016, https://jillstein.nationbuilder.com/recount (last visited Dec. 12, 2016); see also Pennsylvania Recount, Jill2016 (last visited Dec. 12, 2016), http://www.jill2016.com/recountpainfo (In Pennsylvania, "[t]he campaign has mobilized over 2,000 concerned voters in more than 300 election districts in some 20 counties to request recounts").

Only 0.82% of Pennsylvania voters cast their ballots for Dr. Stein, who does not allege that a recount might change the election results. See Unofficial Returns, supra. Indeed, she reportedly has denied that she seeks to change the results. Rather, she reportedly has said that her efforts are intended to ensure that every vote counts. See Jill Stein, Why the Recount Matters: Jill Stein, USA TODAY (Dec. 1, 2016, 3:56 p.m.), http://www.usatoday.com/story/opinion/2016/12/01/election-recount-voter-registration-hacking-jill-stein/94631360.

Dr. Stein has challenged the integrity of the Pennsylvania election results. As alleged, during the November 8 election, the Commonwealth allowed its citizens to cast votes on Direct Recording Electronic (DRE) machines, and used optical-scan machines to tabulate paper ballots. Fifty-four Pennsylvania Counties used one of six DRE machine models. (See Defs.' Resp. Ex. D-1, Doc No. 42-1.) Seventeen Counties used paper ballots that were then counted using optical-scan machines. (See id.) Four Counties used both DRE and optical-scan machines. (See id.) Plaintiffs—both here and in a multitude of Pennsylvania State Courts and Election Boards—have alleged that because these machines might be vulnerable to hacking and cyberattacks, Plaintiffs must be permitted to conduct a forensic analysis of the machines. (See, e.g., Compl. ¶¶ 1-5, Doc. No. 1 ("A majority of machines voted for Donald Trump in Pennsylvania. But who did the people vote for? Absent this Court's intervention, Pennsylvanians will never know that truth.").) With Dr. Stein's financial, legal, and organizational support, Pennsylvania voters have

pursued these claims in judicial and administrative proceedings across the Commonwealth. (See Maazel Decl. Exs. 1-13, 16, 21-22, 24-37, Doc. Nos. 9-1 to 9-13, 9-16, 9-21 to 9-22, 9-24 to 9-40.)

A. Pennsylvania's Election Code

State law sets out the procedures by which voters may contest an election. See 25 P.S. §§ 3291, 3351, 3456; 42 Pa. C.S. § 764. To initiate an election contest, one hundred or more voters must file a petition in the Pennsylvania Commonwealth Court within twenty days after Election Day and supplement that petition with at least five affidavits that the "election was illegal and the return thereof not correct." 25 P.S. §§ 3456–3457. The petitioners must also post a bond "conditioned for the payment of all costs which may accrue in said contested nomination or election proceeding." Id. § 3459.

Pennsylvania law provides two additional methods by which voters may seek a recount and recanvass. First, voters may petition their County Board of Elections. See id. § 3154(e). County Board petitions must be supported by affidavits from three voters in an individual precinct that fraud or error not apparent on the face of the returns has occurred. See id. The petition must be filed "prior to the completion of the computation of all of the returns for the county." Id. If the Board rejects the request for recount or recanvass, the aggrieved petitioners may appeal the Board's decision to the Common Pleas Court. See id. § 3157(a); Rinaldi v. Ferrett, 941 A.2d 73, 76-77 (Pa. Commw. Ct. 2007).

Second, voters may petition the Common Pleas Court for a recount or recanvass. See 25 P.S. §§ 3261–3262. Three voters in the same precinct must verify that fraud or error not apparent from the returns was committed in the vote tabulation. See id. § 3261(a). These petitioners must remit a $50 cash payment or a $100 bond. See id. § 3262(b.2). Unless the

petitioners plead fraud or error with particularity and offer prima facie evidence supporting that allegation, they must also file qualified petitions in every single precinct in which ballots were cast for the office in question. See id. § 3263(a)(1)(i)-(ii). To contest a statewide election in the Common Pleas Court without evidence of fraud, three petitioners must file affidavits from voters in over nine thousand precincts. (See Pls.' Br. 12-13, Doc. No. 5.) These petitions must be filed within five days after completion of the County Board's computation of the vote. See 25 P.S. § 3263(a)(1); Rinaldi, 941 A.2d at 77.

B. Commonwealth Court Election Contest

On Monday, November 28, 2016—the last possible day under Pennsylvania law to bring a contest proceeding—Pennsylvania voters organized by Dr. Stein and represented by her counsel in the instant case filed in Commonwealth Court an election contest, alleging that they had "grave concerns about the integrity of electronic voting machines used in their districts" because of the possibility that the machines could have been hacked. (Maazel Decl. Ex. 37, Doc. No. 9-40 (Nov. 28, 2016 Petition).) The petition was without any of the five required affidavits, was some two pages in length, and did not include any allegation that hacking had actually occurred. (See id.) In light of the rapidly approaching federal safe harbor date, the Commonwealth Court set a hearing for Monday, December 5, 2016 at 10:00 a.m, and ordered the petitioners to post a $1,000,000 bond no later than December 5 at 5:00 p.m. (after the hearing). (See Intervenors' Resp. Ex. 3, Doc. No. 38-2 (Nov. 29, 2016 Order).) The Court stated that it would modify the amount of the bond for good cause. (See id.)

The petitioners never asked the Commonwealth Court to reduce the size of the bond. Instead, on December 3, 2016, they voluntarily withdrew their action, explaining that they could not "afford to post the $1,000,000 bond required by the Court." (Maazel Decl. Ex. 40, Doc. No.

9-43 (Praecipe to Discontinue and Withdraw).) Plaintiffs' Counsel did not dispute before me that the $1,000,000 bond "was effectively a decision not to allow . . . a recount." (Hr'g Tr. 31:14-22.)

C. Other Pennsylvania Recount Efforts

As an extension of the Commonwealth Court suit, on November 28, many voters filed recount and recanvass petitions with their County Boards. (See, e.g., Maazel Decl. ¶ 3 & Ex. 3 ¶ 9, Ex. 6 ¶ 4, Ex. 11 ¶ 15, Ex. 12 ¶ 9, Ex. 13 ¶ 5, Ex. 24 ¶ 3, Ex. 25 ¶ 4, Doc. Nos. 9, 9-3, 9-6, 9-11 to 9-13, 9-24 to 9-25; Lieb Decl. ¶ 5, Doc. No. 7.) Later that day, Defendant Jonathan Marks, Pennsylvania's Commissioner of the Bureau of Commissions, Elections, and Legislation, directed County Boards to accept or reject petitions in accordance with state law. (See Maazel Decl. Ex. 34, Doc. No. 9-37); 25 P.S. §§ 3154(e), 3263(a).

Across the Commonwealth, many County Boards, including Delaware, Lancaster, and Northampton, rejected untimely petitions. (See Maazel Decl. Ex. 11 ¶ 16, Ex. 12 ¶ 16, Ex. 13 ¶ 8, Ex. 25 ¶ 7, Doc. Nos. 9-11 to 9-13, 9-25.) Dr. Stein is currently appealing unfavorable County Board decisions to the Lancaster and Northampton Common Pleas Courts. See Pennsylvania Recount, Jill2016, http://www.jill2016.com/recountpainfo (last visited Dec. 12, 2016). Philadelphia, Allegheny, and Lehigh Counties have since completed their recanvasses, and Chester County has concluded its hand recount. (See Maazel Decl. Exs. 35, 44, Doc. Nos. 9-38, 9-47; Hr'g Tr. 90:1-9); Pennsylvania Recount, supra.

No State Court has ordered the forensic review of the electronic voting machines that Dr. Stein seeks, however. The Philadelphia and Allegheny County Common Pleas Courts both rejected Dr. Stein's appeals from County Board decisions denying the forensic examination. See In re Recount and/or Recanvass of the Vote for President of the United States and for United

States Senate in the November 8, 2016 General Election, No. GD 16-023824 (Pa. C.P. Ct. Allegheny Cty. Dec. 8, 2016); Stein v. Phila. Cty. Bd. of Elections, No. 161103335 (Pa. C.P. Ct. Phila. Cty. Dec. 7, 2016). In Philadelphia, Judge Fletman explained that Pennsylvania law "simply does not mandate or allow a candidate 'to perform a forensic examination of the DRE electronic voting system,'" and that she would "not impose requirements the Legislature has not seen fit to establish," particularly where "there is absolutely no evidence of any voting irregularities." Stein, No. 161103335, at 4. Dr. Stein also directly petitioned the Montgomery County Common Pleas Court, which dismissed the petition. (See Maazel Decl. Exs. 31, 42, Doc. Nos. 9-31, 9-45 (Nov. 30, 2016 Hearing Transcript and Order).)

At this time, six or seven County Boards and Courts were still considering recount petitions. (See Hr'g Tr. 8:20-9:11.) Only one actual recount was pending. (See Hr'g Tr. 90:1-9, 121:20-22.)

D. The Instant Suit

On December 5, 2016, Plaintiffs Dr. Stein and Randall Reitz (a Pennsylvania voter and party to the withdrawn Commonwealth Court action) filed the instant Complaint against Commonwealth Secretary Pedro A. Cortés and Commissioner Jonathan Marks, who oversee election administration. (See Compl. ¶¶ 11-12, Doc. No. 1; Reitz Decl. ¶ 9, Doc. No. 9-2.) In what might be described as scattershot allegations, Plaintiffs bring § 1983 claims that Defendants have violated their right to vote, in violation of the Equal Protection Clause, Substantive Due Process, and the First Amendment. (See Compl. ¶¶ 1-6, Doc. No. 1.) Plaintiffs ask me to declare several sections of the Pennsylvania Election Code unconstitutional, and to issue a preliminary injunction ordering Defendants to "institute an immediate recount of paper ballots,"

and permitting Plaintiffs to conduct a "thorough, forensic examination of a reasonable sample of DRE voting systems." (See Compl. at 18-19, Doc. No. 1 (prayer for relief).)

On December 6, 2016, I granted the unopposed Motion to Intervene filed by President-elect Donald J. Trump, Vice President-elect Michael Pence, their Pennsylvania Electors, Donald J. Trump for President, Inc., and the Republican Party. (See Doc. Nos. 2, 22.) That same day, Plaintiffs filed the instant Motion for a preliminary injunction, asking me to order a recount. (See Pls.' Mot., Doc. No. 4; Pls.' Br., Doc. No. 5.) In accordance with my December 6 Case Management Order, on December 8, 2016, Defendants and Intervenors responded. (Doc. Nos. 23, 38, 38-1, 42.)

I held an evidentiary hearing on December 9, 2016, at which Plaintiffs and the Commonwealth each called an expert witness. As I describe below, I credit the Commonwealth's expert and partially discredit the expert called by Plaintiffs. During the hearing, Plaintiffs narrowed their request for relief: they now seek a hand recount of all paper ballots of one precinct in each of the seventeen paper-ballot Counties and a forensic review of the election management systems of six Counties, including Philadelphia. (See Hr'g Tr. 121:18-22, 122:10-13.) Plaintiffs explained at the hearing that they base their Motion on the purported inadequacies of Pennsylvania's recount procedures, and the Commonwealth's use of electronic voting machines that may be susceptible to hacking.

1. *Recount Procedures*

Plaintiffs contend that the denials by the Commonwealth Court, County Boards, and Common Pleas Courts of their recount petitions amount to violations of their fundamental right to vote. (See Pls.' Br. 28-34, Doc. No. 5.) Plaintiffs challenge the constitutionality of seven

provisions of the Pennsylvania Election Code as applied to their efforts to obtain recounts and recanvasses:

- The requirement that they post a $1,000,000 bond to proceed with the Commonwealth Court contest proceeding. See 25 P.S. § 3459.
- The requirement that a County Board recount petition be supported by verified affidavits from three voters in each precinct. See id. § 3154(e).
- The deadline for County Board recount petitions. See id.
- The requirement that a Common Pleas recount petition must be supported by verified affidavits from three voters in each precinct. See id. §§ 3261(a), 3262(a)(i).
- The filing-fee requirement for Common Pleas recount petitions. See id. §§ 3261(b), 3262(a)(i).
- The deadline for Common Pleas recount petitions. See id. §§ 3262(f), 3263(a)(i).
- The requirement that Common Pleas recount petitions include a qualified petition from all precincts unless a petition pleads a particular act of fraud or error. See id. § 3263(a)(1)(i).

2. *Use of Electronic Voting Machines*

In 1980, Pennsylvania amended its Election Code to permit the use of DRE machines. See 25 P.S. §§ 3031.3, *et seq*. The Code requires the Commonwealth Secretary to "examine and re-examine voting machines" and to make a determination as to whether they meet federal standards and can be safely used. Id. §§ 2621(b), 3031.5(a). In 2012, Secretary Cortés's predecessor certified each of Pennsylvania's six DRE machine models as reliable and secure. (See Hr'g Ex. D-6.) The Secretary similarly certified as safe Pennsylvania's optical-scan machines. See 25 P.S. §§ 2621(b), 3031.5(a). Plaintiffs allege that these certifications notwithstanding, the DRE and optical-scan machines' possible vulnerabilities have abrogated their right to vote.

E. Related Litigation

Dr. Stein has also sought recounts in Michigan and Wisconsin. In Michigan, the State Board of Canvassers initially ordered a recount to begin on December 7. Dr. Stein asked the Michigan District Court to order the State to begin its recount two days sooner. See Compl., Stein v. Thomas, No. 16-14233, Doc. No. 1 (E.D. Mich. Dec. 2, 2016). On December 5, Judge Goldsmith granted the injunction, and the Sixth Circuit affirmed the following day. See Stein v. Thomas, No. 16-14233, Doc. No. 16 (E.D. Mich. Dec. 5), aff'd, No. 16-2690, 2016 WL 7131508, at *3 (6th Cir. Dec. 6, 2016). On December 6, an intermediate state appeals court ruled, however, that because Dr. Stein was not "an aggrieved party" under Michigan law, she had no legal right to request a recount. Judge Goldsmith then promptly dissolved the injunction he had issued. See Thomas, No. 16-14233, Doc. No. 36 (E.D. Mich. Dec. 7, 2016). In rejecting Dr. Stein's allegation that Michigan used vulnerable electronic voting machines, Judge Goldsmith explained:

> Plaintiffs have not presented evidence of tampering or mistake. Instead, they present speculative claims going to the vulnerability of the voting machinery—but not actual injury. Because mere potentiality does not amount to a claim that the vote was not fairly conducted, Plaintiffs' new claims are insufficient to maintain the existing TRO.

Id. at 7. On December 9, the Michigan Supreme Court upheld the lower court's ruling respecting Dr. Stein's lack of standing, thus precluding any Michigan recount. See Trump v. Bd. of State Canvassers, No. 154868 (Mich. Dec. 9, 2016).

On December 1, the Wisconsin Election Commission ordered Dr. Stein's requested recount to begin. See Compl. ¶ 12, Great Am. PAC v. Wis. Elections Comm'n, No. 16-795, Doc. No. 1 (W.D. Wis. Dec. 1, 2016). That day, three political action committees sought to

enjoin the recount. See id. On December 9, the Wisconsin District Court refused to issue an injunction. See Great Am. PAC, No. 16-795, Doc. Nos. 36-37 (W.D. Wis. Dec. 9, 2016).

II. Legal Standards

"[A] preliminary injunction is an extraordinary and drastic remedy, one that should not be granted unless the movant, *by a clear showing*, carries the burden of persuasion." Mazurek v. Armstrong, 520 U.S. 968, 972 (1997) (per curiam) (quoting 11A Wright & Miller, Fed. Prac. & Proc. § 2948 (2d ed. 1995)); see Fed. R. Civ. P. 65(a). "A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." Winter v. Natural Res. Def. Council, Inc., 555 U.S. 7, 20 (2008) (citations omitted). The moving party bears the "heavy burden" of showing that these elements weigh in favor of a preliminary injunction. Republican Party of Pa. v. Cortés, No. 16-5524, 2016 WL 6525409, at *3 (E.D. Pa. Nov. 3, 2016) (citing Ferring Pharms., Inc. v. Watson Pharms., Inc., 765 F.3d 205, 210 (3d Cir. 2014), and Punnett v. Carter, 621 F.2d 578, 588 (3d Cir. 1980)).

Because Plaintiffs seek an injunction that "is mandatory and will alter the status quo," they "must meet a higher standard of showing irreparable harm in the absence of the injunction." Bennington Foods LLC v. St. Croix Renaissance, Grp., LLP, 528 F.3d 176, 179 (3d Cir. 2008).

The Federal Rules of Evidence do not strictly apply during preliminary injunction proceedings. I must exercise discretion in "weighing all the attendant factors, including the need for expedition, to assess whether, and to what extent, affidavits or other hearsay materials are appropriate given the character and objectives of the injunctive proceeding." Kos Pharms., Inc. v. Andrx Corp., 369 F.3d 700, 719 (3d Cir. 2004) (internal quotation marks and citation omitted).

III. Standing

Defendants and Intervenors argue that Plaintiffs lack standing to bring the instant suit. (See Intervenors' Resp. 16-17, Doc. No. 38-1; Defs.' Resp. 13-17, Doc. No. 42; Hr'g Tr. 99:7-100:19.) I agree.

The "existence of a case or controversy is a prerequisite to all federal actions, including those for declaratory or injunctive relief." Belitskus v. Pizzingrilli, 343 F.3d 632, 639 (3d Cir. 2003) (quoting Phila. Fed'n of Teachers v. Ridge, 150 F.3d 319, 322-23 (3d Cir. 1998)); see also U.S. Const., Art. III § 2 (jurisdiction of federal courts limited to "Cases" or "Controversies"). To make out Article III standing,

> a plaintiff must show (1) that it has suffered an "injury in fact" that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.

Friends of the Earth, Inc. v. Laidlaw Envtl. Svcs. (TOC), Inc., 528 U.S. 167, 180-81 (2000) (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992)). The "party invoking federal jurisdiction bears the burden of establishing" standing. Wittman v. Personhuballah, 136 S. Ct. 1732, 1737 (2016) (quoting Lujan, 504 U.S. at 561).

At the December 9 hearing, Intervenors argued persuasively that Plaintiffs lack standing. (See Hr'g Tr. 99:7-100:19.) Remarkably, Plaintiffs did not respond. Even though Dr. Stein was present and could have testified as to why she is an aggrieved party with standing to seek a recount, she was not called.

The allegations in Plaintiffs' Complaint respecting standing are less than clear. They allege that Pennsylvania's DRE machines are "vulnerable, hackable, [and] antiquated," that the Pennsylvania Election Code's recount provisions are "labyrinthine, incomprehensible, and

impossibly burdensome," and that neither Dr. Stein nor her voters have been permitted to examine the machines. (See Compl. ¶¶ 1-5, 63, 82, Doc. No. 1.) But see 25 P.S. § 3031.14(b)(2) (allowing each party on the ballot to be present during testing and "to make independent tests of the equipment prior to, during, and following the vote count"). Significantly, although Plaintiffs apparently question whether Pennsylvania votes were correctly counted, they do not so allege. (See Compl. ¶ 4, Doc. No. 1 ("Were Pennsylvania votes counted accurately? That truth is not difficult to learn.").) Finally, Plaintiffs make no factual allegations respecting Mr. Reitz other than that he "is a voter in the State of Pennsylvania, and voted in the 2016 presidential election." (Id. ¶ 10.) These allegations are insufficient to confer standing.

Neither Plaintiff has alleged that she or he has suffered an actual injury. Dr. Stein is not a Pennsylvania voter and does not allege that a recount will change the Pennsylvania vote total in her favor. Although Mr. Reitz is a Pennsylvania voter, he has not alleged that his vote was inaccurately recorded or tallied in the final Pennsylvania vote count. Plaintiffs' allegation that voting machines may be "hackable," and the seemingly rhetorical question they pose respecting the accuracy of the vote count, simply do not constitute injury-in-fact. See, e.g., Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1148 (2013) (the plaintiffs' standing argument, which "rest[ed] on their highly speculative fear" of government surveillance and "on a highly attenuated chain of possibilities," did not satisfy injury requirement); Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (after payroll processor's database was hacked, the plaintiffs' allegations that their personal information could be misused "rel[ied] on speculation" and did not constitute injury-in-fact).

It also appears that Plaintiffs seek to protect the rights of all Pennsylvania voters. (See, e.g., Compl. ¶ 101, Doc. No. 1 ("Defendants . . . have deprived and severely

burdened . . . Pennsylvania voters, including Plaintiff Randall Reitz, of their fundamental right to vote.").) There is no authority to support such an invocation of standing. See Cty. Ct. of Ulster Cty., N.Y. v. Allen, 442 U.S. 140, 155 (1979) ("As a general rule, if there is no constitutional defect in the application of the statute to a litigant, he does not have standing to argue that it would be unconstitutional if applied to third parties in hypothetical situations." (citing Broadrick v. Oklahoma, 413 U.S. 601, 610 (1973))); Broadrick, 413 U.S. at 610-11 ("[C]onstitutional rights are personal and may not be asserted vicariously. . . . Constitutional judgments . . . are justified only out of the necessity of adjudicating rights in particular cases between the litigants brought before the Court.").

The Supreme Court's reasoning here is instructive:

> First, the Court has held that when the asserted harm is a "generalized grievance" shared in substantially equal measure by all or a large class of citizens, that harm alone normally does not warrant exercise of jurisdiction. Second, even when the plaintiff has alleged injury sufficient to meet the "case or controversy" requirement, this Court has held that the plaintiff generally must assert his own legal rights and interests, and cannot rest his claim to relief on the legal rights or interests of third parties. Without such limitations . . . the courts would be called upon to decide abstract questions of wide public significance even though other governmental institutions may be more competent to address the questions and even though judicial intervention may be unnecessary to protect individual rights.

Warth v. Seldin, 422 U.S. 490, 499-500 (1975) (citations omitted)); see also Oh v. Phila. Cty. Bd. of Elections, No. 08-81, 2008 WL 4787583, at *7 (E.D. Pa. Oct. 31, 2008) ("The prudential principles support that [a losing candidate] cannot rest his claim to relief on the legal rights or interests of the voters. The claim plaintiff alleges on behalf of these voters, even if substantiated, would amount to a '"generalized grievance" shared in substantially equal measure by all or a large class of citizens' and is not sufficient to confer standing." (quoting Warth, 422 U.S. at 499)). Cf. Pa. Psychiatric Soc'y v. Green Spring Health Svcs., Inc., 280 F.3d 278, 288 & n.10 (3d Cir. 2002) (suggesting that plaintiff "candidates for public office may be able to assert the

rights of voters," but only where the plaintiff herself suffers an injury and voters are "hindered from asserting [their] own rights and share[] an identity of interests with the plaintiff").

Finally, Plaintiffs have not shown that the extraordinary relief they seek—a hand recount of a sample of paper ballots in optical-scan Counties and a forensic examination of six Counties' election management systems—will redress their alleged injuries. Dr. Stein received less than 1% of the vote in Pennsylvania and does not allege that the recount and forensic examination will yield the votes necessary for her to prevail in Pennsylvania's election. Mr. Reitz voted on a DRE machine in Montgomery County and has not explained how a forensic examination of a sample of County election management computer systems would vindicate his individual right to vote. (See Reitz Decl. ¶¶ 2, 15, Doc. No. 9-2.) There is no evidence before me even suggesting that a recount or audit of any kind would confirm whether the vote of Mr. Reitz or anyone else was counted inaccurately, or would somehow correct an inaccurately recorded vote.

In sum, because Plaintiffs have alleged speculative injuries that are not personal to them and could not be redressed by the relief they seek (or any relief I could order), they are without standing to bring their claims.

Given the significance of this matter, I will fully discuss all the alternative grounds on which I base my denial of Plaintiffs' Motion.

IV. Jurisdiction

Even if Plaintiffs had standing, their State Court recount efforts raise serious questions about my jurisdiction to consider their claims.

A. Rooker-Feldman Doctrine

In 1923, the Supreme Court held that federal courts may not "exercis[e] jurisdiction over a case that is the functional equivalent of an appeal from a state court judgment." Marran v.

Marran, 376 F.3d 143, 149 (3d Cir. 2004) (citing D.C. Ct. of Appeals v. Feldman, 460 U.S. 462 (1983) and Rooker v. Fidelity Trust Co., 263 U.S. 413 (1923)). This doctrine applies where: (1) the federal plaintiff lost in state court; (2) the plaintiff complains of injuries caused by a state court judgment; (3) that judgment was rendered before the federal suit was filed; and (4) the plaintiff is inviting the district court to review and reject the state judgment. See Exxon Mobil Corp. v. Saudi Basic Indus. Corp., 544 U.S. 280, 284 (2005); Great W. Mining & Mineral Co. v. Fox Rothschild LLP, 615 F.3d 159, 166 (3d Cir. 2010) (identifying the second and fourth requirements as key to the Rooker-Feldman inquiry). Rooker-Feldman extends to actions brought by parties in privity with the parties in the state action. See Marran, 376 F.3d at 151. State Court judgments include interlocutory orders and orders of lower state courts. Pieper v. Am. Arbitration Ass'n, Inc., 336 F.3d 458, 462 (6th Cir. 2003). I must consider "whether the injury complained of in federal court existed prior to the state-court proceedings and thus could not have been 'caused by' those proceedings." Great W. Mining & Mineral Co., 615 F.3d at 167.

As I have described, on November 28, 2016, voters organized by Dr. Stein, including Mr. Reitz, initiated an election contest in the Commonwealth Court. (See Maazel Decl. Ex. 37, Doc. No. 9-40.) They based their petition on the same expert opinion they offer here: that there exists the theoretical possibility that Pennsylvania's voting machines may have been hacked. (See id.) They asked the Court to order "a full recount of the 2016 Presidential Election in all counties in the Commonwealth to determine the true winner of that Election." (Id.) Petitioners asked the Court to set bond at $25,000. (See id.) On December 2, 2016, the Commonwealth Court ordered the petitioners to post a $1,000,000 bond, causing them to withdraw their contest petition. (See Maazel Decl. Ex. 39, Doc. No. 9-42 (Dec. 2, 2016 Order); id. Ex. 40, Doc. No. 9-43 (Dec. 3, 2016 Praecipe to Discontinue and Withdraw) ("Petitioners are citizens of ordinary

means. They cannot afford to post the $1,000,000 bond required by the Court. Accordingly, kindly mark the above captioned matter withdrawn and discontinued.").)

It appears that the four Rooker-Feldman abstention criteria have been met. As Plaintiffs' Counsel acknowledged during the December 9 hearing, the Commonwealth Court's December 2 order was an adverse state court decision. (See Hr'g Tr. 31:11-22 ("The Commonwealth Court's decision to require a million dollar bond was effectively a decision not to allow . . . a recount.")); see also Hagerty v. Succession of Clement, 749 F.2d 217, 219-20 (5th Cir. 1987) (adverse ruling requirement read expansively to include state court procedural rulings). Plaintiffs certainly complain of injuries caused by the Commonwealth Court's decision, which was rendered before they filed the instant suit. Finally, Plaintiffs are inviting me to review and reject the Commonwealth Court's decision. Indeed, the legal memorandum they have submitted here is undoubtedly the same as the appellate brief they would have filed, had Plaintiffs chosen to appeal the Commonwealth Court's decision to the Pennsylvania Supreme Court.

Courts discussing Rooker-Feldman abstention have repeatedly explained that it is intended to preclude unsuccessful State Court litigants from "appealing" unfavorable State Court rulings to federal courts. See, e.g., Marran, 376 F.3d at 149. Yet, that is just what Plaintiffs seek to do here: ask me to "overrule" the Commonwealth Court's effective refusal to order a recount. Rooker-Feldman compels me to abstain.

B. Younger Abstention

District courts have discretion to "abstain from exercising jurisdiction over a particular claim where resolution of that claim in federal court would offend principles of comity by interfering with an ongoing state proceeding." Lazaridis v. Wehmer, 591 F.3d 666, 670 (3d Cir. 2010) (per curiam) (citing Middlesex Cty. Ethics Comm. v. Garden State Bar Ass'n, 457 U.S.

423, 437 (1982)); Addiction Specialists, Inc. v. Twp. of Hampton, 411 F.3d 399, 408 (3d Cir. 2005). Younger abstention is proper where: (1) there are ongoing state judicial proceedings involving the federal plaintiff; (2) the state proceedings implicate important state interests; and (3) the state proceedings afford an adequate opportunity to raise the federal claims. See Lazaridis, 591 F.3d at 670. Abstention is particularly appropriate where the requested equitable relief would "render the state court's orders or judgments nugatory." Schall v. Joyce, 885 F.2d 101, 108 (3d Cir. 1989).

1. *Ongoing State Judicial Proceedings*

Under Younger, the appellate review available to the State Court plaintiffs constitutes an ongoing proceeding. See, e.g., Laurel Sand & Gravel, Inc. v. Wilson, 519 F.3d 156, 166 (4th Cir. 2008) (applying Younger to State Court appeal of administrative proceeding); Maymo-Melendez v. Alvarez-Ramirez, 364 F.3d 27, 35 (1st Cir. 2004) (same); Majors v. Engelbrecht, 149 F.3d 709, 713 (7th Cir. 1998) (same); see also Huffman v. Pursue, Ltd., 420 U.S. 592, 608 (1975) ("Virtually all of the evils at which Younger is directed would inhere in federal intervention prior to completion of state appellate proceedings.").

Plaintiffs confirmed at the December 9 hearing that Dr. Stein has initiated multiple state recounts, and that "six or seven" County Boards and Common Pleas Courts were still considering their recount petitions. (Hr'g Tr. 8:20-9:11); see also Pennsylvania Recount, Jill2016, http://www.jill2016.com/recountpainfo (last visited Dec. 12, 2016) (indicating Dr. Stein is appealing from Lancaster and Northampton County's decisions). Further, the Allegheny and Philadelphia Common Pleas Courts' denials of forensic audits are ripe for appeal. See Pa. R.A.P. 903(c).

In these circumstances, the first Younger prong has been satisfied.

2. *Important State Interests*

The Commonwealth has an obvious interest in regulating the conduct of its elections. See, e.g., Timmons v. Twin Cities Area New Party, 520 U.S. 351, 366 (1997) (maintaining stability of political system during election); Anderson v. Celebrezze, 460 U.S. 780, 798 (1983) (voter education); Storer v. Brown, 415 U.S. 724, 735 (1974) (avoiding political fragmentation during election); Green Party of Pa. v. Aichele, 89 F. Supp. 3d 723, 751 (E.D. Pa. 2015) (preserving the integrity of the nomination process); Petition of Berg, 713 A.2d 1106, 1109 (Pa. 1998) (managing ballot size and ensuring statewide support for candidates); Cavanaugh v. Schaeffer, 444 A.2d 1308, 1311-12 (Pa. Commw. Ct. 1982) (ensuring serious candidacies).

In analyzing this requirement, however, I must "adequately examine the facts and claims alleged in the federal and state actions." Addiction Specialists, Inc., 411 F.3d at 410 (citing Gwynedd Props., Inc. v. Lower Gwynedd Twp., 970 F.2d 1195, 1203 (3d Cir. 1992)). The threshold question is whether enjoining the state court's enforcement of the Election Code, if granted, would be tantamount to invalidating the Election Code provisions themselves. See Addiction Specialists, Inc., 411 F.3d at 410-11.

The state court petitioners seek the same relief Plaintiffs seek here: recounts of votes counted by optical-scan machines and a forensic review of DRE machines. Plaintiffs here are thus effectively asking me to nullify the Pennsylvania Election Code provisions applied by the State Courts and Boards, and to annul the unfavorable judgments issued by these bodies. Cf. Gwynedd Props., Inc., 970 F.2d at 1201 (abstention not appropriate where "federal plaintiff seeks only prospective relief without seeking to annul state court judgments").

Finally, there is no suggestion that Plaintiffs may not raise in the Pennsylvania Courts the same constitutional claims they have raised here. Plainly they can. See, e.g., Petition of Berg,

713 A.2d 1106 (Pa. 1998); Trinsey v. Mitchell, 625 A.2d 49 (Pa. 1993); Cavanaugh v. Schaeffer, 444 A.2d 1308 (Pa. Commw. Ct.), aff'd, In re Cavanaugh, 444 A.2d 1165 (Pa. 1982) (per curiam).

In sum, because any decision I render on Plaintiffs' constitutional claims will impinge upon the existing state proceedings, I will abstain under Younger.

V. Delay

As I have described, despite the December 13 certification deadline, Plaintiffs waited until November 28 to proceed in Commonwealth Court and until December 5 to proceed here. That delay has caused what Judge Pappert recently described as a "judicial fire drill" and what I recently described as a "mad scramble"—unnecessary and unfair to all concerned. Pa. Democratic Party v. Republican Party of Pa., No. 16-5664, 2016 WL 6582659, at *5 (E.D. Pa. Nov. 7, 2016); Republican Party of Pa. v. Cortés, No. 16-5524, 2016 WL 6525409, at *4 (E.D. Pa. Nov. 3, 2016). Contrary to Plaintiffs' suggestions, the December 9 hearing underscored the absence of any good reason for their delay. Plaintiffs base this action on Pennsylvania's use of electronic machines to tabulate votes and the recount provisions of its Election Code. The Commonwealth's use of electronic machines began well before the 2016 election. Optical-scan machines have been in use for decades. See Banfield v. Cortés, 110 A.3d 155, 159 (Pa. 2015). Pennsylvania's use of DRE machines was the subject of nine years of State Court litigation. See id. at 155, 160-65, 178. Plaintiffs' expert witness acknowledged at the December 9 hearing that he knew before the 2016 election all the information on which he based his opinion respecting the DRE machines' purported vulnerabilities. (See Hr'g Tr. 27:10-16.) The recount procedures that Plaintiffs challenge were largely enacted in 1937. See Pennsylvania Election Code, Act of June 3, 1937, Pub. L. No. 1333, art. I §§ 101, *et seq.* (codified as amended at 25 P.S. §§ 2600, *et*

seq.). Once again, in the run up to Election Day, Dr. Stein had the right under the Election Code to be present or to have a technical expert be present on her behalf, for the testing of the voting machines and the counting of the ballots. See Stein v. Phila. Cty. Bd. of Elections, No. 161103335, at 3 (Pa. C.P. Ct. Phila. Cty. Dec. 7, 2016) (citing 25 P.S. §§ 2650, 3031.14(b)(2)). She chose not to avail herself of that right.

The only relevant fact unknown to Plaintiffs before the election was its outcome. Yet, Dr. Stein then waited nearly three weeks, until November 28, to file the Commonwealth Court contest petition and the County Board recount petitions. (See Maazel Decl. Ex. 37, Doc. No. 9-40.) During the December 9 hearing, Plaintiffs' Counsel was unable to offer a credible justification for this delay. Once again, even though Dr. Stein was present and could have explained under oath her reasons for delay, she did not do so.

Having effectively been denied a recount in Commonwealth Court, Plaintiffs filed the instant suit on December 5. As I explain below, if that delay makes it impossible for the Commonwealth to certify its Electors by tomorrow, all of Pennsylvania's six million voters could be disenfranchised. Courts have repeatedly held that such prejudicial and unnecessary delay alone provides ample grounds to deny the emergency injunctive relief Plaintiffs seek. See, e.g., Santana Prods., Inc. v. Bobrick Washroom Equip., Inc., 401 F.3d 123, 135 (3d Cir. 2005); Pa. Democratic Party, 2016 WL 6582659, at *5 (collecting cases); see also Crookston v. Johnson, 841 F.3d 396, 398 (6th Cir. 2016) ("Call it what you will—laches, the Purcell principle, or common sense—the idea is that courts will not disrupt imminent elections absent a powerful reason for doing so."). I am compelled to reach the same conclusion here. Plaintiffs are not entitled to the "emergency" relief they seek because they have inexcusably waited well past the eleventh hour to seek it.

VI. Entitlement to Injunctive Relief

The December 9 hearing confirmed that Plaintiffs have not met any of the requirements for the mandatory injunctive relief they seek.

A. Likelihood of Success on the Merits

Plaintiffs contend that Pennsylvania's use of electronic voting machines raises concerns of tampering, and its "Election Code, as applied by defendants and the [E]lection [B]oards, poses such barriers to verifying the vote as to deny the people of Pennsylvania the fundamental right to have their vote counted." (Pls.' Br. 27, Doc. No. 5.) Plaintiffs have failed to demonstrate a likelihood of prevailing on the merits of these claims.

"When the state legislature vests the right to vote for President in its people, the right to vote as the legislature has prescribed is fundamental." Bush v. Gore, 531 U.S. 98, 104 (2000) (per curiam). The right to vote necessarily includes the right to have the vote fairly counted. See Reynolds v. Sims, 377 U.S. 533, 554 (1964) ("[Q]ualified voters have a constitutionally protected right . . . to have their votes counted. (citing United States v. Mosley, 238 U.S. 383, 386 (1915))); United States v. Classic, 313 U.S. 299, 315 (1941) (right to vote includes right of "qualified voters within a state to cast their ballots and have them counted"). Due process may be implicated "[i]f the election process itself reaches the point of patent and fundamental unfairness." Griffin v. Burns, 570 F.2d 1065, 1077 (1st Cir. 1978); see also Marks v. Stinson, 19 F.3d 873, 888 (3d Cir. 1994) ("[R]ejection of a ballot where the voter has been effectively deprived of the ability to cast a legal vote implicates federal due process concerns.").

The right to have one's vote counted does not, however, encompass the right to have one's vote verified through a mandatory statewide recount. As Judge Goldsmith explained in rejecting Dr. Stein's Michigan recount suit, "[t]here is no case law recognizing an independent

federal right to a recount that either this Court or the parties have come across, in the absence of actual deprivation of voting rights." See Thomas, No. 16-14233, Doc. No. 36 at 7 (E.D. Mich. Nov. 7, 2016). Plaintiffs' Counsel conceded as much at the December 9 hearing. (See Hr'g Tr. 37:4-11.)

No authority suggests otherwise. Courts have explained ballot access restrictions can "limit the field of candidates from which voters might choose." Anderson v. Celebrezze, 460 U.S. 780, 786 (1983) (quoting Bullock v. Carter, 405 U.S. 134, 143 (1972)); Belitskus v. Pizzingrilli, 343 F.3d 632, 643 (3d Cir. 2003) (same); Const. Party of Pa. v. Cortés, 116 F. Supp. 3d 486, 501 (E.D. Pa. 2015) (same). Recount restrictions impose no such burden.

Due process limitations on the manner by which elections may be conducted are also separate from any "right" to a mandatory recount. The (rare) decisions that sustain due process challenges to elections involve documented instances of improperly cast ballots, wholesale refusal to count properly cast ballots, direct infringements of the right to cast ballots, or a total failure to conduct the election. See Marks, 19 F.3d at 887 ("massive absentee ballot fraud, deception, intimidation, harassment and forgery," and "many of the absentee votes were tainted"); Griffin, 570 F.2d at 1074 (state refused to count "the absentee and shut-in ballots that state officials had offered to the voters"); Bonas v. Town of N. Smithfield, 265 F.3d 69 (1st Cir. 2001) (failure to hold election required by town charter); Duncan v. Poythress, 657 F.2d 691 (5th Cir. Unit B Sept. 1981) (refusal to call special election required by state law); see also League of Women Voters of Ohio v. Brunner, 548 F.3d 463, 478 (6th Cir. 2008) (sustaining due process challenge where "voters were denied the right to vote because their names were missing from the rolls," "[p]oll workers improperly refused assistance to disabled voters," and "[p]rovisional ballots were not distributed to appropriate voters"). Due process was impugned in these cases

because the challenged government actions had impaired or outright barred voters from casting a first, constitutionally protected ballot.

Plaintiffs base their § 1983 claims on their contention that the Pennsylvania Election Code's recount restrictions, taken together, impose a "severe" burden on their right to vote and are not "narrowly drawn to advance compelling state interests." (Pls.' Br. 30, Doc. No. 5 (citing Belitskus, 343 F.3d at 643).) I do not agree. Pennsylvania's recount procedures are not impermissibly "arbitrary or unreasonable." Stein v. Thomas, No. 16-2690, 2016 WL 7131508, at *3 (6th Cir. Dec. 6, 2016). "[T]here must be a substantial regulation of elections if they are to be fair and honest and if some sort of order, rather than chaos, is to accompany the democratic processes." Storer v. Brown, 415 U.S. 724, 730 (1974). Concomitant with the principles of federalism, Pennsylvania has developed its own statutory framework by which voters may challenge elections, a framework courts have applied for decades without any hint that the required procedures might violate the Constitution. See, e.g., Olshansky v. Montgomery Cty. Election Bd., 412 A.2d 552 (Pa. 1980) (bond provision); In re Recount of Ballots Cast in General Election on Nov. 6, 1973, 325 A.2d 303 (Pa. 1974) (time limits and verification requirement); Pfuhl v. Coppersmith, 253 A.2d 271 (Pa. 1969) (verification provision); Appeal of Bradley, 42 A.2d 155 (Pa. 1945) (time limits); In re Pazdrak's Contested Election, 137 A. 109 (Pa. 1927) (verification provision). The "reasonable, nondiscriminatory restrictions" on initiating recounts serve an "important regulatory interest": ensuring that election challenges are swiftly and fairly resolved to preserve "the integrity of the vote." Burdick v. Takushi, 504 U.S. 428, 434 (1992) (quoting Anderson, 460 U.S. at 788)); (see also Pa. Senate Majority Caucus *Amicus* Br. 4, Doc. No. 46.)

Finally, the Election Code's procedures may seem burdensome to Plaintiffs because they needlessly waited three weeks—until November 28—to initiate their statewide recount campaign. Their most significant protest that is unrelated to timing and deadlines is the $1,000,000 bond order by the Commonwealth Court. Yet, the Court stated that it would change the bond amount "upon good cause shown." (Intervenors' Resp. Ex. 4, Doc. No. 38-2 (Dec. 2, 2016 Order).)

In these circumstances, Plaintiffs have not shown a likelihood that they will prevail on the merits of their constitutional claims.

B. Immediate Irreparable Harm

I agree with Plaintiffs that tampering with the Pennsylvania vote totals would violate the right to vote itself and constitute an irreparable harm. See Council of Alt. Political Parties v. Hooks, 121 F.3d 876, 883 (3d Cir. 1997) (infringement on voting rights "cannot be alleviated after the election"); Williams v. Salerno, 792 F.2d 323, 326 (2d Cir. 1986) (voters "would certainly suffer irreparable harm if their right to vote were impinged upon"); Marks v. Stinson, 1994 WL 47710, at *13-14 (E.D. Pa. Feb. 18) (violation of right to vote in free and fair election constituted irreparable harm), rev'd in part on other grounds, 19 F.3d 873 (3d Cir. 1994). Plaintiffs have presented no credible evidence, however, that any such tampering occurred or could occur; the Commonwealth presented compelling evidence that it did not.

As I have described, for decades, Pennsylvania has had in place extensive laws and protocols intended to ensure the integrity of the vote. At the December 9 hearing, the Commonwealth called Dr. Michael Shamos, who was deeply involved in the creation and monitoring of Pennsylvania's voting security procedures. (See Hr'g Tr. 45:22-46:13; Hr'g Ex. D-5 ¶ 6.) With a Yale computer science Ph.D. and a law degree, Dr. Shamos is an expert in

electronic voting, the electronic voting provisions of the Pennsylvania Election Code, and computer science. (See Hr'g Tr. 44:23-45, 45:18-19, 73:5-8; Hr'g Ex. D-5 ¶ 2.)

Plaintiffs seem to suggest that Pennsylvania's votes are recorded and tabulated statewide by a single computer that is Internet-accessible and susceptible to tampering. As Dr. Shamos made clear, however, this simply is not so. (See Hr'g Tr. 59:10-24, 60:17-61:2.)

Plaintiffs also base their voting security allegations on the possibility that "malware" might have been secretly installed in Pennsylvania voting and vote tabulation machines, thus corrupting Pennsylvania's voting results. Dr. Shamos made clear, however, that, given Pennsylvania's highly dispersed system of taking and tabulating votes and the numerous integrity checks provided by law and practice, no such "hack" could be effected.

The Commonwealth employs many thousands of DRE machines (4,200 in Allegheny County alone). (See Hr'g Tr. 62:20-24.) Before Pennsylvania's DRE machines are first put into use, independent testing authorities check them for malware. (See Hr'g Tr. 62:12-24.) These authorities also conduct "a forensic examination of the code" for any software updates for the DRE machines. (Hr'g Tr. 74:4-17.) The Commonwealth again tests the machines before each election; any machine with a malware infection will fail the test. (See Hr'g Tr. 49:13-16.) If malware is on the machine after the election, examiners may compare "hash functions" to determine if the "malware is still there." (Hr'g Tr. 49:23-50:3.) Even if the malware were specially programmed (as Plaintiffs conjure) to activate only on Election Day and delete itself when its work concludes (a programming feat Dr. Shamos has never seen accomplished), it would be detected by "parallel testing"—a process by which County employees conduct a simulated test vote on specially sequestered machines. (Hr'g Tr. 49:16-22, 55:22-56:20.)

Allegheny County conducted parallel testing during the 2016 election and did not report any irregularities. (See Hr'g Tr. 85:15-20.)

Dr. Shamos also described the insuperable logistical difficulties involved in installing malware on each of Pennsylvania's many thousands of DRE machines. Because DREs do not connect to the Internet, hackers cannot upload malware onto them remotely. (See Maazel Decl. Ex. 1, Doc. No. 9-1 (Halderman Aff. ¶ 18).) Physically hacking DREs to influence an election is practically impossible. Each machine is sealed by Commonwealth voting officers. (See Hr'g Tr. 50:9-11.) It would take substantial time to open a DRE, hack it, close it, and apply counterfeit seals. (See Hr'g Tr. 50:11-13.) In Dr. Shamos's view, it is less than implausible to suggest that anyone secretly could hack Pennsylvania's DREs without being noticed. (See Hr'g Tr. 50:9-20 (estimating "it would take four months" to hack all of Allegheny County's DRE machines).)

Dr. Shamos credibly explained that any attempts to place malware onto the DRE machines through other methods would also fail. Portable Election Ballots (PEBs)—small cartridges that carry ballot templates and are connected to DRE machines on Election Day—are removable media that could theoretically carry malware to the DRE machines. PEBs cannot be used to hack the machines while the polls are open, however. (See Hr'g Tr. 51:19-20, 53:6-12, 53:23-54:7, 54:4-8.) Furthermore, the PEBs do not connect to the Internet; instead, they connect only to each County's central election management computer system, which is turned on only "a few times a year" and does not connect to the Internet. (Hr'g Tr. 51:8-11.) Indeed, it is illegal under Pennsylvania law to connect those County computer systems to the Internet. (See Hr'g Tr. 76:4-11.)

Moreover, because each Pennsylvania County uses a different central election management computer system, there is no single location through which hackers could introduce

malware that would infect all of Pennsylvania's DRE machines. (See Hr'g Tr. 59:21-24, 60:17-61:2.) Instead, hackers would have to attack separately the systems of each of the fifty-four Counties that use DRE machines.

Finally, Dr. Shamos clearly and credibly explained that suggestions of foreign hacking influencing the 2016 Election—including President Obama's December 9 referral of such hacking for investigation by the Central Intelligence Agency—related only to email servers and the like, and so had nothing to do with the integrity of Pennsylvania's voting machines. (See Hr'g Tr. 58:24-59:9.)

Although Dr. Shamos acknowledged the theoretical possibility that an individual DRE machine could be hacked, he credibly explained that in light of all of the protections in place, the suggestion of widespread hacking borders on the irrational. (See Hr'g Tr. 63:23-64:9 ("The [vote tampering] scenarios that have been posited are approximately as likely as the fact that androids from outer space are living amongst us and passing as humans.").)

In contrast, Plaintiffs' computer science expert, Dr. J. Alex Halderman, although qualified as a computer science "expert," knew virtually nothing about Pennsylvania's security procedures, the practices of the Commonwealth's election officials, or the Pennsylvania Election Code. Dr. Halderman admitted that he had "no evidence" that any voting machine was hacked, and that the election outcome was "probably not" the result of a hack. (Hr'g Tr. 25:22-26:1, 26:19-24.) Insofar as Dr. Halderman opined that even though it was "more likely than not that there was no hack," there remains a "significant possibility" that a hack occurred, I discredit that contradictory testimony. (Hr'g Tr. 17:3-6, 29:5-11.) Unlike Dr. Shamos, who based his opinions on Pennsylvania's actual practices and requirements, Dr. Halderman based his opinion on public media reports of possible hacking in Illinois and Arizona, and hacking of the

Democratic National Committee's email server before the election. (See Hr'g Tr. 17:7-24; see also Maazel Decl. Ex. 1, Doc. No. 9-1 (Halderman Aff. Exs. B-D, F, H).) Once again, these media reports do not remotely relate to Election Day hacks of offline voting machines in Pennsylvania. (See Hr'g Tr. 58:24-59:9.)

Plaintiffs submitted the reports of four other experts, each of whom opined only that Pennsylvania's DRE machines were vulnerable to hacking, not that any hacking actually occurred. (See Hursti Aff. ¶ 15, Doc. No. 10 ("These DRE machines are ***susceptible*** to fraud and tampering." (emphasis added)); Lopresti Aff. ¶ 11, Doc. No. 11 ("The DRE Machines are unreliable and ***susceptible*** to tampering and fraud." (emphasis added)); Buell Aff. ¶ 2, Doc. No. 12 ("In my opinion, the electronic voting system used by Allegheny County . . . is ***vulnerable*** to malicious interference and inadvertent error." (emphasis added)); Hoke Aff. ¶ 9, Doc. No. 13 ("The DRE Machines Used In Pennsylvania Are ***Vulnerable***." (emphasis added)).) One of Plaintiffs' experts averred that optical-scan machines could also theoretically be hacked, but did not provide any evidence to suggest that they were. (See Hursti Aff. ¶¶ 40-58, Doc. No. 10.) Even if I were to credit these opinions, they make out little more than the theoretical possibility a voting machine somewhere in the Commonwealth might be susceptible to tampering.

There can be no more serious challenge to an election than the suggestion that the votes cast were dishonestly recorded. Yet, "Plaintiffs have not made out even the possibility—much less the likelihood"—that any vote tampering occurred in Pennsylvania during the 2016 election. Pa. Republican Party v. Pa Democratic Party, No. 16-5664, 2016 WL 6582659, at *7 (E.D. Pa. Nov. 7, 2016). Plaintiffs have certainly not made the required "clear showing of immediate irreparable injury." ECRI v. McGraw-Hill, Inc., 809 F.2d 223, 226 (3d Cir. 1987) (quoting Cont'l Grp., Inc. v. Amoco Chems. Corp., 614 F.2d 351, 359 (3d Cir. 1980)). In these

circumstances, I must deny their request for a mandatory injunction.

C. The Balance of Equities and Public Interest

Because these factors are intertwined, I consider them together. Plaintiffs contend that the equities weigh in their favor because "many voters will effectively be denied the right to vote" without a recount. (Pls.' Br. 39, Doc. No. 5.) As I have discussed, however, Plaintiffs have raised only spectral fears that machines were hacked or votes miscounted. Against these unreasoning concerns, I must balance the real risk that the twelfth hour recount recount order that Plaintiffs seek would disenfranchise six million Pennsylvanians. Once again, Plaintiffs seek a hand recount of all paper ballots cast in one precinct in each of the seventeen optical-scan Counties (except for Chester County) and a forensic review of the election management systems of six Counties, including Philadelphia. (See Hr'g Tr. 121:18-122:1, 122:10-13.) I credit Dr. Shamos's testimony that it would take a "long day" to count the seventeen precincts of paper ballots that Plaintiffs have requested. (Hr'g Tr. 126:17-24.) Before the recount can begin, however, each County Board (none of which is a Party here) must find, hire, and train individuals to conduct the recount. (See Hr'g Tr. 124:10-15, 127:3-15.) All of this obviously cannot be completed before December 13 (tomorrow)—the date by which Pennsylvania's Presidential election results must be certified. I also credit Dr. Shamos's testimony that no meaningful forensic review of election management systems could conclude by tomorrow evening. Significantly, Dr. Halderman testified that the forensic examination would take at least two days. (Hr'g Tr. 123:12-17.) Even if I were to credit that testimony, Plaintiffs' own expert confirmed that ordering the forensic audit would preclude Pennsylvania's compliance with the December 13 certification requirement. See 3 U.S.C. § 5. If Pennsylvania does not certify its election results by tomorrow, it is likely that the selection of the Commonwealth's electors will

devolve to the State Legislature. See U.S. Const., Art. II § 1, cl. 2 ("Each State shall appoint, in such Manner as the Legislature thereof may direct, a Number of Electors . . . ."). This would abrogate the right of millions of Pennsylvanians to select their President and Vice President. Plaintiffs' requested relief may thus be unconstitutional. See Bush v. Gore, 531 U.S. 98, 110 (2000) (per curiam) (suspending recount because Florida could not devise constitutional recount procedures to conclude vote tabulation before expiration of the federal safe harbor).

In these circumstances the equities and public interest conclusively weigh against granting Plaintiffs' Motion.

VII. Conclusion

Dr. Stein has repeatedly stated that she has sought a Pennsylvania recount to ensure that every vote counts. Granting her later than last minute request for relief, however, could well ensure that no Pennsylvania vote counts. Such a result would be both outrageous and completely unnecessary; as I have found, suspicion of a "hacked" Pennsylvania election borders on the irrational. Finally, Plaintiffs' claims for relief suffer from several flaws, each fatal to their Motion. For all these reasons, I will deny that Motion.

An appropriate Order follows.

/s/ Paul S. Diamond

December 12, 2016 Paul S. Diamond, J.

IN THE COMMONWEALTH COURT OF PENNSYLVANIA

Mark Banfield, Sarah Beck, Joan Bergquist, Alan Brau, Lucia Dailey, Peter Deutsch, Constance Fewlass, Barbara Glassman, Marijo Highland, Janis Hobbs-Pellechio, Deborah Johnson, Andrew McDowell, James Michaels, J. Whyatt Mondesire, Mary Montresor, Rev. James Moore, Cathy Reed, Regina Schlitz, Alexander Sickert, Daniel Sleator, Susanna Staas, Stephen J. Strahs, Mary Vollero, Jeanne Zang, Petitioners	:	
v.	:	No. 442 M.D. 2006
Carol Aichele, Secretary of the Commonwealth, Respondent	:	

BEFORE: HONORABLE BONNIE BRIGANCE LEADBETTER, Judge

OPINION NOT REPORTED

MEMORANDUM OPINION BY JUDGE LEADBETTER **FILED: October 1, 2013**

The Secretary of the Commonwealth (Secretary) seeks summary relief on the six counts (out of ten) remaining undecided in the action by twenty-four individual voters,[1] who seek an order in mandamus directing the Secretary to de-

[1] Specifically, Petitioners are Mark Banfield, Sarah Beck, Joan Bergquist, Alan Brau, Lucia Dailey, Peter Deutsch, Constance Fewlass, Barbara Glassman, Marijo Highland, Janis Hobbs–Pellechio, Deborah Johnson, Andrew McDowell, James Michaels, J. Whyatt Mondesire, Mary **(Footnote continued on next page…)**

certify specific electronic voting systems (DREs) currently used in some counties in the Commonwealth.[2] For the reasons that follow, the motion is granted.

This is the fourth time this case is before the court. Previously, we denied the Secretary's preliminary objections to the petition for review. *See Banfield v. Cortes (Banfield I)*, 922 A.2d 36 (Pa. Cmwlth. 2007) (en banc), permission to appeal denied by Supreme Court order dated December 16, 2008 (70 MM 2007). Thereafter, we also denied the Petitioners' motion for partial summary judgment on Counts I (DREs fail to provide a permanent physical record), IV (DREs fail to provide for a recount as required under the Pennsylvania Election Code[3]), VI (Secretary failed to perform a required reexamination of the DREs), IX (certification process violates the equal protection clause, Article I, § 26 of the Pennsylvania Constitution), and X (certification process violates the uniformity requirement in Article VII, § 6 of the Pennsylvania Constitution). *See Banfield v. Aichele (Banfield II)*, 51 A.3d 300 (Pa. Cmwlth. 2012) (en banc). Subsequently, based on the rationale underpinning the rulings in *Banfield II*, the court dismissed Counts I, IV, V, VI and, dismissed as moot Count VI inasmuch as the Secretary performed the reexamination sought therein. *See Banfield v. Aichele*, No. 442 M.D. 2006, Order filed January 29, 2013. Presently, the Secretary seeks summary relief on Count II (DREs susceptible to fraud), Count III (certification procedures

---

(continued...)

Montresor, Rev. James Moore, Cathy Reed, Regina Schlitz, Alexander Sickert, Daniel Sleator, Susanna Staas, Stephen J. Strahs, Mary Vollero and Jeanne Zang.

[2] The voting machines subject to this challenge are: the ELECTronic 1242, made by Danaher Industrial Controls; the AccuVote TSX, made by Diebold Election Systems, Inc. (now Dominion); the iVotronic, made by Elections Systems & Software, Inc.; the eSlate, made by Hart InterCivic, Inc.; the AVC Edge II and the AVC Advantage, made by Sequoia Voting Systems, Inc. (now Dominion).

[3] Act of June 3, 1937, P.L. 1333, *as amended*, 25 P.S. §§ 2600-3591.

inadequate), Count VII (testing procedures inadequate), Count VIII (likely failure to count all votes accurately in violation of Article I, § 5 of the Pennsylvania Constitution concerning free and equal elections), Counts IX and X (equal protection and uniformity violations of state constitution).[4]

In Counts II, III and VII, Petitioners seek relief based on failure to comply with certain requirements imposed under Section *1107-A of the Election* Code, added by the Act of July 11, 1980, P.L. 600, 25 P.S. § 3031.7. The pertinent provisions of Section 1107-A direct:

> No electronic voting system shall, upon examination or reexamination, be approved by the Secretary of the Commonwealth, or by any examiner appointed by him, unless it shall be established that such system, at the time of such examination or reexamination:
>
> . . . .
>
> (11) Is suitably designed for the purpose used, is constructed in a neat and workmanlike manner of durable material of good quality, is safely and efficiently useable

---

[4] Summary relief in the form of a judgment in favor of the Secretary may be granted only in those cases "where the record clearly shows that there are no genuine issues of material fact and that the moving party is entitled to judgment as a matter of law." *P.J.S. v. Pa. State Ethics Comm'n*, 555 Pa. 149, 153, 723 A.2d 174, 176 (1999). Moreover, "[w]hen resolving a motion for summary judgment, the record must be viewed in the light most favorable to the opposing party, and all doubts as to the existence of a genuine issue of material fact must be resolved in favor of the nonmoving party." *Id.*

Pursuant to Pa. R.A.P. 1532 this court may, upon application, enter summary relief "at any time after the filing of a petition for review" if the right of the applicant is clear. In the present case, the court ordered discovery to be completed by March 7, 2013. *See* Order dated January 29, 2013. Nonetheless, Petitioners have filed a motion to compel production of documents containing over 642 communications that Respondents redacted or withheld, which remains pending. See Motion to Compel the Production of Documents filed March 15, 2013. Having reviewed these documents in camera, it is apparent that the additional documents and information sought by Petitioners will not yield evidence that the machines fail to comply with the statutory requirements for accuracy and security.

> in the conduct of elections and, with respect to the counting of ballots cast at each district, is suitably designed and equipped to be capable of absolute accuracy, which accuracy shall be demonstrated to the Secretary of the Commonwealth.
>
> (12) Provides acceptable ballot security procedures and impoundment of ballots to prevent tampering with or substitution of any ballots or ballot cards.
>
> (13) When properly operated, records correctly and computes and tabulates accurately every valid vote registered.
>
> . . . .
>
> (16) If the voting system is of a type which provides for the computation and tabulation of votes at the district level, the district component of the automatic tabulating equipment shall include the following mechanisms or capabilities:
>
> . . . .
>
> (iii) It shall be so constructed and controlled that, during the progress of voting, it shall preclude every person from . . . tampering with the tabulating element.
>
> . . . .

25 P.S. § 3031.7 (11) -(13), (16)(iii). In addition, subsection (17)(i) of 1107-A, 25 P.S. § 3031.7(17)(i), imposes the same tamper-proof requirement to systems that compute and tabulate votes at a central counting center. Essentially, Petitioners aver that the challenged DREs are not capable of the required accuracy and are not sufficiently tamper-proof, that the Secretary's testing procedures fail to ensure full compliance with all of the statutory requirements listed above and that the Secretary has failed in her duty to adopt adequate testing procedures.

In general, mandamus is available only to a plaintiff who establishes a clear legal right to compel the official performance of a ministerial act or mandatory duty and there is no other adequate remedy at law. *Banfield I*, 922 A.2d

at 42. In the present case, where mandamus is not sought based on the Secretary's failure to certify DREs as required under the Election Code but on the premise that she failed to properly exercise her discretion in the performance of this duty, Petitioners must establish that the Secretary performed her statutory duties arbitrarily, fraudulently or under a mistake of law. *Id.* The standard for affording mandamus relief does not encompass a review of the Secretary's discretion in how she performed her duties so as to impose the court's view as to how these duties should be performed. *Maxwell v. Bd. of Dirs. Sch. Dist. of Farrell*, 381 Pa. 561, 566, 112 A.2d 192, 195 (1955): *Chadwick v. Dauphin County Office of the Coroner*, 905 A.2d 600, 604 (Pa. Cmwlth. 2006). To a large degree, this inappropriate oversight is exactly what Petitioners seek.

In their brief, Petitioners characterize their cause of action as "a case about how closely the court will monitor the executive's performance of its duty - entrusted to it by the legislature - to ensure the integrity of elections." Petitioners' Brief in Opposition to Summary Relief at 23. While this court has recognized its responsibility to protect the Commonwealth's interest in the integrity of the election process, *In re Carlson,* 430 A.2d 1210, 1212 (Pa. Cmwlth. 1981), that does not mean that courts have broad authority to prescribe the best way for the Secretary to perform her duties. *See Banfield I,* 922 A.2d at 44 (domain of the judiciary is to interpret, construe and apply the law). In order to prevail in their quest to de-certify the challenged DREs, Petitioners must establish that the DRE voting systems actually fall short of the statutory requirements for accuracy and security from tampering. *See Davidowitz v. Philadelphia County*, 324 Pa. 17, 187 A. 585 (1936) (in a challenge to use of "voting machines" the court refused to enjoin their use absent a clear legislative or constitutional violation). To survive

the present motion for summary judgment in favor of the Secretary, the record must contain some evidence that would support such a finding. *See Young v. Dep't of Transp.*, 560 Pa. 373, 376, 744 A.2d 1276, 1277 (2000). In this case, where the subject of inquiry, i.e., the workings of electronic voting systems, is outside the skill and knowledge of the ordinary layman, Petitioners cannot prevail in their cause of action without supportive expert opinion. *Id.* at 376, 744 A.2d at 1278. Petitioners have come forward with no evidence that the challenged machines fail to accurately record votes when properly used. Rather, review of the expert reports discloses that Petitioners can establish no more than that a possibility exists that the challenged DREs could in theory be subject to tampering or human error. But in this regard the challenged systems do not differ from any other voting system.

On behalf of Petitioners, Dr. Daniel Lopresti, a Professor and Chair of the Department of Computer Science and Engineering at Lehigh University, opined that the Secretary's certification process was inadequate in that it failed to give sufficient attention to security vulnerabilities identified in three studies that are well known in the field. Specifically, Lopresti points to the program tampering accomplished during a laboratory challenge conducted at Princeton University, known as the "Hursti exploit," the detailed source code and penetration testing that revealed security vulnerabilities in California's "Top to Bottom Review," and similar vulnerabilities demonstrated in Ohio's "EVEREST study." Petitioners' Exh. 18 in Opposition to Summary Relief, Lopresti Report at 6-8. These studies demonstrate vulnerabilities, worthy perhaps of consideration in the evolution of technological improvements, but the possibility that tampering can produce inaccuracy does not render the DREs incapable of the absolute accuracy required under the Election Code. Capability and vulnerability are not mutually exclusive

characteristics, i.e., capable of accuracy does not mean invulnerable to tampering. Furthermore, the fact that these studies uncovered vulnerability does not establish the presence of unacceptable security procedures. Testing machine vulnerabilities does not fully test security procedures that encompass not only tamper-proofing built into the electronics but also measures to check and cross-check human activity in the conduct of elections.

Similarly, Petitioners' expert, Dr. Douglas W. Jones, a Professor at the University of Iowa, opined that the challenged DREs' software is a "systematic source of security vulnerabilities" rendering the DREs not suitably designed for the purpose used and not constructed in a workmanlike manner. Petitioners' Exh. 22 in Opposition to Summary Relief, Jones Report at ¶¶ 29 – 40. Jones's expert report, while noting specific vulnerabilities identified in the California and Ohio studies, does not conclude that the machines are incapable of doing what they are designed to do – count and tabulate votes. Vulnerability to tampering or manipulation exists now and has existed since voting began. In his report, Jones recognized that:

> Secure voting is very difficult, whether done using manual, mechanical or electronic means. While the algorithms involved are trivial, requiring nothing more than a sum, for each candidate or ballot position, of the number of votes, the distributed nature of the computation and the number of participants pose immense problems. Elections involve an appreciable fraction of the entire national population as participants, and the history of election fraud includes examples that were perpetrated by every class of participant, from voter to polling place election judge to election administrator to voting system maintenance technician.

Jones Report at ¶ 18. Indeed, even paper ballots can be destroyed or altered if those with access to the voting and tabulation process are intent on fraudulent manipulation of results, perhaps even more easily than electronic machines since

no technical expertise is required. Since voting will always be vulnerable to fraud, a mere possibility of a security breach is not alone sufficient to warrant overriding the Secretary's determination to certify the systems. While the expert reports call attention to perceived problems, they do not establish that the machines used successfully for many elections are necessarily fatally flawed.

Furthermore, the identification of certain vulnerabilities discovered in tests conducted in California or Ohio does not establish that the Secretary's testing was fatally defective. There is not a dispute here as to whether the DREs are imperfect; the challenged DREs, as well as the electronic voting systems the Petitioners point to as preferable, are imperfect. There is also no dispute that testing procedures are not, and cannot be, perfect. However, the present cause of action fails nonetheless because the experts have failed to establish that the Secretary's testing procedures and the DREs that she certified create more than a mere possibility of error in recording and tabulating votes. If the mere possibility of such error were considered sufficient to bar use of a voting system then we would be left with none.

Courts confronted with similar challenges based on the possibility of vote miscount have reached similar conclusions. As the court in *Weber v. Shelley*, 347 F.3d 1101 (9th Cir. 2003), observed:

> No balloting system is perfect. Traditional paper ballots, as became evident during the 2000 presidential election, are prone to over-votes, under-votes, hanging chads, and other mechanical and human errors that may thwart voter intent. . . . The unfortunate reality is that the possibility of electoral fraud can never be *completely* eliminated, no matter which type of ballot is used.

Id. at 1106 – 7 (emphasis in original). In *Wexler v. Anderson*, 452 F.3d 1226 (11th Cir. 2006), the court indicated that *likelihood or probability* of vote miscount, *not*

its mere possibility, is required to trigger strict scrutiny of state recount procedures, stating that:

> Plaintiffs' fundamental error is one of perspective. By adopting the perspective of the residual voter [i.e., a voter who upon a recount will have his paper or optical scan ballot examined manually for voter intent], they avoided the question that is of constitutional dimension: Are voters in touchscreen counties less likely to cast an effective vote than voters in optical scan counties?
>
> . . . .
>
> [I]f voters in touchscreen counties are burdened at all, that burden is the mere possibility that should they cast residual ballots, those ballots will receive a different, and allegedly inferior, type of review in the event of a manual recount.

Id. at 1231-32. In *Hennings v. Grafton*, 523 F.2d 861 (7th Cir. 1975), the court opined that, "[T]he failure of election officials to take statutorily prescribed steps to diminish what was at most a theoretical possibility that devices might be tampered with . . . fall[s] far short of constitutional infractions." *Id.* at 864. This court is firmly persuaded that more than a mere possibility of inaccuracy or insecurity is required to justify the relief Petitioners seek.

Further, Counts VIII,[5] IX[6] and X[7] allege that the inadequate testing and improper certification of the DREs allows for the use of systems that fail to

---

[5] Count VIII alleges that certification of the challenged DREs "create the risk that persons for whom the majority of voters have not cast their ballots will be declared the election winners and will take office, in contravention of the very essence of our democracy." Petition for Review at 32, ¶ 134. Petitioners maintain that this transgresses the guaranty in Article I, § 5 of the Pennsylvania Constitution that: "Elections shall be free and equal; and no power, civil or military, shall at any time interfere to prevent the free exercise of the right of suffrage."

[6] Count IX alleges that certification of the challenged DREs "threatens Petitioners' fundamental right to vote because the voting systems' defects and security flaws create the risk that Petitioners, together with other Pennsylvania voters, have their votes rendered meaningless or, worse yet, deemed cast for a candidate for whom they did not vote." Petition for Review at 33, ¶ 138. Petitioners assert that this interference with the right to vote violates the guaranty in

(Footnote continued on next page...)

ensure that votes will be honestly captured and counted as cast, thus interfering with the Petitioners' fundamental right to vote and discriminating against those forced to use the challenged DREs. Petitioners' Brief in Opposition to Summary Relief at 47. These constitutional challenges, based as they are on the premise that the challenged DREs are so inaccurate and insecure as to infringe on the right to vote and the requirement for uniform election regulation, cannot survive inasmuch as Petitioners are unable to prove their starting premise.

Accordingly, the Secretary's application for summary relief is granted.

Bonnie B. Leadbetter

BONNIE BRIGANCE LEADBETTER,
Judge

(continued...)

Article I, § 26 of the Pennsylvania Constitution that: "Neither the Commonwealth nor any political subdivision thereof shall deny to any person the enjoyment of any civil right, nor discriminate against any person in the exercise of any civil right."

[7] Count X alleges that: "Because the likelihood of an inaccurate tally that cannot be audited is greater in counties using the certified DRE voting systems than in counties that use systems that permit independent recounts upon an allegation of error or fraud, the use of the certified DRE voting systems threatens to create an imbalance in the weight given to the votes in the various counties, thereby depriving all Pennsylvania citizens, including Petitioners of the uniformity rights and equal protection rights secured under the Pennsylvania Constitution." Petition for Review at 35, ¶ 144. Petitioners assert that this violates the prescription in Article VII, § 6 that: "All laws regulating the holding of elections by the citizens . . . shall be uniform throughout the state."

IN THE COMMONWEALTH COURT OF PENNSYLVANIA

Mark Banfield, Sarah Beck, Joan Bergquist, Alan Brau, Lucia Dailey, Peter Deutsch, Constance Fewlass, Barbara Glassman, Marijo Highland, Janis Hobbs-Pellechio, Deborah Johnson, Andrew McDowell, James Michaels, J. Whyatt Mondesire, Mary Montresor, Rev. James Moore, Cathy Reed, Regina Schlitz, Alexander Sickert, Daniel Sleator, Susanna Staas, Stephen J. Strahs, Mary Vollero, Jeanne Zang, Petitioners	:	
v.	:	No. 442 M.D. 2006
Carol Aichele, Secretary of the Commonwealth, Respondent	:	

ORDER

AND NOW, this 1st day of October, 2013, Respondent's Application for Summary Relief is granted. Judgment in favor of the Respondent shall be *entered* on Counts II, III, VII, VIII, IX and X of the Petition for Review.

Bonnie B. Leadbetter

BONNIE BRIGANCE LEADBETTER,
Judge

Certified from the Record

OCT - 1 2013

and Order Exit