STATE OF WISCONSIN CIRCUIT COURT DANE COUNTY

JILL STEIN,
c/o Emery Celli Brinckerhoff & Abady LLP
600 Fifth Avenue, 10th Floor
New York, NY 10020,

Petitioner,

Case No.:

Case Code: 30607

v.

WISCONSIN ELECTIONS COMMISSION,
212 East Washington Avenue
Third Floor
Madison, WI 53707,

Respondent.

PETITION FOR JUDICIAL REVIEW UNDER WIS. STAT. CHAPTER 227 OR, ALTERNATIVELY, CERTIORARI REVIEW OR OTHER APPROPRIATE RELIEF

Jill Stein, by her undersigned attorneys, hereby files this petition and alleges as follows:

INTRODUCTION

1. Petitioner Jill Stein was the Green Party's presidential candidate in the 2016 election. Petitioner requested a recount of the votes for President in Wisconsin. During the recount process, on December 6, 2016 Petitioner requested "access to the software components that were used to record and tally the votes in the election," pursuant to Wis. Stat. § 5.905(4).

2. Wis. Stat. § 5.905(4) provides that upon request by a party to a recount, the Wisconsin Elections Commission ("Elections Commission") must "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 confidentiality of all proprietary information to which the person is provided access."

3. The Elections Commission issued a final decision on March 15, 2018 disposing of Petitioner's request. *See* Ex. 1 (March 15, 2018 Decision of the Wisconsin Elections Commission). That decision granted Petitioner certain access to the software code as required by Wis. Stat. § 5.905(4). However, the Elections Commission's decision denied Petitioner sufficient access to the software by restricting the amount of time her designees may spend reviewing the code, purporting to restrict the methodologies of analysis Petitioner's designees may perform with respect to the code, and limiting the purposes for which Petitioner may use her access—powers the Commission does not possess under the statute. The decision further fails to permit Petitioner and her designees to access certain categories of software that indisputably were "used to record and tally the votes in the election."

4. Petitioner accordingly brings this petition for judicial review to secure her clear legal right to meaningful access to the election software under Wis. Stat. § 5.905(4).

PARTIES

5. Petitioner Jill Stein was the Green Party nominee for President of the United States in the 2016 election.

6. Respondent Wisconsin Elections Commission is an agency of the State of Wisconsin, which is endowed by statute with the responsibility for the administration of all laws relating to elections and election campaigns. *See* Wis. Stat. § 5.05.

FACTUAL ALLEGATIONS

7. On November 25, 2016, Petitioner filed with the Elections Commission a sworn petition for a recount of votes cast in the State of Wisconsin for President of the United States in the 2016 election.

8. The Elections Commission approved the petition, and the recount proceeded over the course of ten days in December 2016.

9. In an email to the administrator of the Elections Commission dated December 6, 2016—while the statewide recount of votes in the presidential election was still underway—Petitioner invoked her right under Wis. Stat. § 5.905(4) to "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" and designated eight experts to undertake the review. *See* Ex. 2 (Dec. 6, 2016 Email from D. Greenberger).

10. The Elections Commission certified the results of Wisconsin's presidential election on December 12, 2016. Prior to certification, in response to an inquiry from Petitioner's counsel, the Elections Commission's administrator stated that "today's certification does not prejudice a candidate's (party to the recount) ability to request access to the software components under Wis. Stat. 5.905(4)." Ex. 3 (Dec. 12, 2016 Email from M. Haas).

11. In the ensuing months, Petitioner's counsel exchanged correspondence with the Elections Commission and with counsel for the state's two predominant election software vendors—Election Systems & Software, LLC ("ES&S") and Dominion Voting ("Dominion") (collectively, the "Vendors")—concerning the logistics of the software review.

12. As part of that process, on February 22, 2017, Petitioner provided the Elections Commission's legal counsel with a proposed confidentiality agreement to govern the review, as

well as a detailed letter explaining her proposals. *See* Ex. 4 (Feb. 22, 2017 Ltr. From D. Greenberger to N. Judnic); Ex. 5 (Redline of Proposed Confidentiality Agreement).

13. Petitioner's draft agreement proposed the following categories of software for inclusion in the review: "all vote-counting source code, modules, scripts, make files, static data files, program comments, and other human-readable computer instructions used to count votes, including without limitation any and all code for (a) any election management software (including without limitation Electionware, GEMS, Unity, WinEDS or Democracy Suite); (b) any software component used to initialize election databases with jurisdiction, voter, and candidate information; (c) any software component used to design the appearance of paper and touchscreen ballots; (d) any software component used to collect, transfer, or tally election results; (e) any software component used to verify election results using audit data; (f) any software component used to control interaction between election management software and voting hardware; and/or (g) any firmware, bootloader components, and/or other software components resident on any hardware or device used to tabulate votes." Ex. 5 ¶ 2. Petitioner's letter noted her position that "the Review must encompass more than just firmware, and must extend to include other components that are used in recording and tallying votes." Ex. 4 at 2.

14. Discussions among Petitioner, the Elections Commission, and the Vendors concerning the proposed software review continued throughout 2017. As part of that discussion, on May 22, 2017, Petitioner's counsel wrote a letter to the Election's Commission's legal counsel reiterating among other things Petitioner's position that the software review should include election management software, database initialization software, ballot design software, vote collection and tallying software, audit verification software, and firmware resident on voting

hardware—all of which are needed to record and tally votes in an election. *See* Ex. 6 (May 22, 2017 letter).

15. The Elections Commission met on June 20, 2018 in closed session to discuss the status of the software access request. At that meeting, the Elections Commission directed its staff to seek independent technical assistance from a third party in making its determination as to which software components should be subject to review under § 5.905(4).

16. Petitioner's request to review the election software pursuant to § 5.905(4) remained pending before the Elections Commission for the balance of 2017.

17. The Elections Commission retained Pro V&V for technical assistance in determining which software components would be subject to review. Pro V&V issued a report dated January 17, 2018. Ex. 9 (January 17, 2018 Pro V&V Report). According to the report, "WEC submitted an encrypted USB drive with all voting systems in use in Wisconsin during the 2016 Presidential Election," Ex. 9 at 3, which Pro V&V reviewed "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," *id.* at 2. Upon information and belief, Pro V&V reviewed only categories of software that had already been placed in escrow by the Vendors, and did not consider whether other software components that were not in escrow "were used to record and tally the votes in the election" and therefore properly should have been included. Pro V&V identified the components it had reviewed and determined to be subject to review only by technical naming conventions without reference to the functions of particular software components. *See id.* at 15-17. Accordingly, Petitioner had no way to assess the accuracy or comprehensiveness of the report or determine which software was being recommended for inclusion in the inspection.

18. On January 31, 2018, the Elections Commission held a special meeting to address Petitioner's request. At that meeting, the Commission made several interim non-final decisions related to Petitioner's request. See Ex. 7 (Feb. 7, 2018 Ltr. From N. Judnic to C. Meuler).

a. First, the Elections Commission adopted a proposed Confidentiality Order drafted by Commission staff to govern the review. Ex. 7; Ex. 8 (Confidentiality Order).

b. Second, the Elections Commission adopted the January 17, 2018 Pro V&V report.

c. Third, the Commission adopted a series of "parameters" to govern Petitioners' software review. Among these parameters was a requirement that Petitioner submit "a written examination plan concerning the specific details of all examinations to be conducted," no later than February 15, 2018. Ex. 7 at 2.

19. Petitioner worked diligently with a preeminent expert to comply with the Elections Commission's directive and submitted a proposed Plan on February 15, 2018. *See* Ex. 10.

20. Petitioner's Plan was developed by Professor Alex Halderman, a computer scientist and leading expert on election security. Dr. Halderman is a Professor of Computer Science and Engineering and the Director of the Center for Computer Security and Society at the University of Michigan in Ann Arbor, Michigan, where he has been a faculty member for nine years. He has a Ph.D., a Master's Degree, and a Bachelor's Degree in Computer Science, all from Princeton University. His research focuses on computer security and privacy, with an emphasis on problems that broadly impact society and public policy. Among his areas of research are software security, data privacy, and election cybersecurity. He has published more than seventy articles and books, and his work has been cited in more than 6,300 scholarly

publications. He has served on the program committees for thirty research conferences and workshops, and he co-chaired the USENIX Election Technology Workshop, which focuses on electronic voting security. He received the John Gideon Award for Election Integrity from the Election Verification Network, the Alfred P. Sloan Foundation Research Fellowship, the IRTF Applied Networking Research Prize, and the University of Michigan College of Engineering 1938E Award for teaching and scholarship. Professor Halderman has published peer-reviewed research analyzing the security of electronic voting systems used in Wisconsin, other U.S. states, and other countries. He was part of a team of experts commissioned by the California Secretary of State to conduct a "Top-to-Bottom" review of the state's electronic voting systems. He has also investigated methods for improving the security of electronic voting, such as efficient techniques for testing whether electronic vote totals match paper vote records. In June 2017, he testified to the U.S. Senate Select Committee on Intelligence regarding cybersecurity threats to U.S. elections.

21. In Petitioner's cover letter enclosing the Plan, counsel noted that the software approved by Pro V&V for inclusion in the review appeared to be insufficient. *See* Ex. 11 (February 15, 2018 Ltr. from C. Meuler).

22. Petitioner's plan was comprehensive and proposed a review based on the principles of Open-Ended Vulnerability Testing ("OEVT"), a protocol for conducting security reviews of electronic voting systems recommended by the Election Assistance Commission's ("EAC") Technical Guidelines Development Committee ("TGDC"). In light of the fact that Pro V&V had approved over 4 million lines of code from eleven different voting machines for inclusion in the review, Petitioner's plan proposed devoting 145 total person-weeks to the review, including 15 total days of on-site code review. *See generally* Ex. 10.

23. On February 26, 2018, the Vendors submitted a letter to the Elections Commission objecting to Petitioner's Plan. *See* Ex. 12 (February 26, 2018 Vendors Ltr.). The Vendors provided no substantive counter-proposal to Petitioner's Plan and suggested that the entire software review—of more than 4 million lines of code—should somehow be completed in one to two days.

24. On March 1, 2018, Petitioner submitted a letter to the Elections Commission responding to the Vendors' objections. *See* Ex. 13 (March 1, 2018 Ltr.).

25. At its March 2, 2018 meeting, the Elections Commission again discussed Petitioner's request. Members of the Commission expressed concern that the Vendors had failed to submit a proposal that was faithful to the statutory mandate of software access, and also expressed the view that Petitioner's proposed Plan might be too expansive. Accordingly, the Commission directed the Vendors and Petitioner to each submit any revised proposals for the software review by March 9, 2018.

26. At the same March 2 meeting, the Elections Commission also approved an updated version of the Pro V&V Report, dated February 12, 2018, in which Pro V&V modified certain of its initial recommendations. *See* Ex. 14 (Feb. 12, 2018 Pro V&V Report). Again, the report listed by technical file path and name a series of software components Pro V&V determined were appropriate for inclusion in Petitioner's software review. The updated report still did not identify the software components by function or otherwise permit Petitioner to understand which software was being included and excluded from the inspection.

27. On March 9, 2018, Petitioner submitted an Alternative Plan for the anticipated software review. *See* Ex. 15 (Alternative Plan). This Alternative Plan proposed a more constrained software review. It contemplated a more limited schedule for the review of only 33

days start-to-finish (compared to 90 in the original Plan). It also reduced the number of person-hours expected to be expended, requesting just 36 on-site person-weeks, with six reviewers.

28. Petitioner submitted a detailed letter enclosing the Alternative Plan which emphasized that OEVT analysis should be permitted and noted that the submission of the Alternative Plan was "without waiving our position that Dr. Stein's original Plan should be approved." *See* Ex. 16 (March 9, 2018 Letter). Petitioner also submitted two expert affidavits explaining why Petitioners' proposals were reasonable from a computer science perspective. *See* Ex. 17 (Halderman Affidavit); Ex. 18 (Appel Affidavit).

29. Dr. Halderman explained that under the Alternative Plan, "the review team will only be able to meaningfully review and analyze the source code for some sub-set of the voting systems that Pro V&V approved for access." Ex. 17 ¶ 10. Accordingly, as explained in Dr. Stein's March 9, 2018 letter, "the alternative request is *below* the minimum needed to meaningfully review all 11 machines." Ex. 16. at 4.

30. The Vendors submitted their own proposal on March 9, 2018. *See* Ex. 19. There were no expert affidavits or testimony submitted with that proposal.

31. On March 13, 2018, the Elections Commission discussed Petitioner's December 2016 request. The Commissioners posed questions to representatives of Petitioner and the Vendor and discussed the relative merits of each proposed software review plan.

THE ELECTIONS COMMISSION'S DECISION MUST BE MODIFIED

32. On March 15, 2018, the Elections Commission issued its final decision granting Petitioner's request to review the software components used in the 2016 election. *See* Ex. 1.

33. This final decision adopted several aspects of Petitioner's Alternative Plan, but rejected other essential elements and thereby deprived Petitioner of meaningful access to the software.

The Decision's Under-inclusive Grant of Software Access Contravenes the Statute

34. First, the decision does not authorize review of all "software components that were used to record and tally the votes in the election," as is mandated by Wis. Stat. § 5.905(4).

35. The Elections Commission adopted the February 12, 2018 report by Pro V&V, which identified particular source code Pro V&V believed qualified for review. The components in question were identified only by technical naming convention, but Petitioner later learned that Pro V&V's proposal did not include election management system ("EMS") source code. *See* Ex. 20 (February 12, 2018 Email from N. Judnic to C. Meuler) (confirming that "there is no EMS code included in the packages.").

36. It is beyond dispute that EMS software is used to record and tally votes. For example, on its website, ES&S describes one election management system, Electionware, as being used to "to create an election information database, format ballots, program voting and ballot scanning equipment, count ballots, review ballot images, and report results."[1] Another ES&S system, Unity, is described as facilitating ballot tabulation "for smooth, continuous ballot scanning from start to finish."[2] A third election management system, GEMS, is described as "automat[ing] the complete election cycle from precinct/district setup, to race definition,

[1] *See* https://www.essvote.com/products/7/26/election-management-software/electionware/

[2] *See* https://www.essvote.com/products/7/14/election-management-software/unity/

tabulation and reporting."[3] Dominion describes its election management system, Democracy Suite, as performing functions "[f]rom election programming and ballot creation to results consolidation and reporting," and notes that it includes a "ballot-level audit trail" that "creates a digital image of every ballot scanned" and "appends to that image a record of how the voter's intent was interpreted by the voting system."[4] Indeed, in its June 29, 2015 letter approving the Democracy Suite system for use in Wisconsin, the Government Accountability Board stated that the Democracy Suite software is used for "Results Tally and Reporting."[5] Given these descriptions of EMS software by both the Vendors and the Elections Commission, the decision's failure to grant Petitioner access to the EMS source code contravenes § 5.905(4).

37. Because EMS code is used to record and tally votes, the Elections Commission erroneously interpreted Wis. Stat. § 5.905(4) by failing to grant Dr. Stein's designees access to EMS code, in addition to the code Pro V&V already identified. And because a correct interpretation of the statute compels the granting of access to all "software components that were used to record and tally the votes in the election," the Elections Commission's decision must be modified pursuant to Wis. Stat. § 227.57(5) to permit access to all such software.

The Decision's Limitations on the Methodology and Purpose of Petitioner's Review Contravene the Statute

38. The final decision also purports to limit the purposes for which Dr. Stein may undertake the software review. In particular, the Elections Commission determined that "[u]se of the OEVT methodology in the process of providing the campaign with access to the voting equipment software components is denied because its objective of testing the security and identifying potential security vulnerabilities in the software components is beyond the scope of

[3] *See* https://www.essvote.com/products/7/39/election-management-software/gems/

[4] *See* http://www.dominionvoting.com/products

[5] *See* http://elections.wi.gov/sites/default/files/page/65/approval_and_certification_letter_dominion_democr_10931.pdf

Wis. Stat. § 5.905." Ex. 1 at 8. The Elections Commission also "specifically denie[d] the campaign's request to implement hypothesis generation and hypothesis testing as outlined in its Alternative Plan." *Id.* at 10.

39. The Elections Commission exceeded its authority by imposing restrictions on what methodology is used to inspect software once statutory access is granted and attempting to circumscribe the purposes for which a software review may be undertaken. The relevant statute provides that a candidate who participates in a recount may "receive access" and that the Elections Commission "shall grant access to the software components to each designated person." Nowhere does the statute limit what such access should entail.

40. The Elections Commission's overly restrictive reading of § 5.905(4) is mistaken as a matter of statutory construction. The statute does not impose any limitations on the purposes for which a candidate may invoke her right to conduct a software review, nor on the methods her designees may use to analyze the software once access is granted. The only requirement the Legislature imposed was that candidates abide by confidentiality obligations to ensure that proprietary information is not disseminated. Had the Legislature wished to impose additional restrictions, it could have done so. The absence of such limitations from the statute is presumptively the product of an intentional legislative decision. *See, e.g.*, *Brauneis v. State, Labor, & Indus. Review Comm'n*, 236 Wis. 2d 27, 42 (2000) ("We should not read into the statute language that the legislature did not put in."); *Ball v. Dist. No. 4, Area Bd. Of Vocational, Technical & Adult Educ.*, 117 Wis. 2d 529, 539 (1984) ("The more reasonable presumption is that the legislature chose its terms carefully and precisely to express its meaning.").

41. Moreover, to the extent the statute is ambiguous, the limitations it imposes on access to the election software code must be construed narrowly. "Statutes in derogation of the

common law are to be narrowly construed." *Rose v. Schantz*, 56. Wis. 2d 222, 227 (1972). The common law recognizes "a general right to inspect and copy public records and documents," and does not "condition enforcement of this right on a proprietary interest in the document or upon a need for it as evidence in a lawsuit." *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589. 597 (1978). Accordingly, laws that seek to shield public records from public review—like the one at issue here[6]—cannot be read to contain implicit restrictions on the review and use of such information that are not plainly apparent from the statutory text. Yet the Elections Commission nonetheless imposed such restrictions.

42. The Elections Commission misinterpreted § 5.905(4) by reading it to bar candidates from using the statutorily-mandated software access to conduct security analysis. The Commission concluded that the statute only permits candidates "to determine whether the tabulator interprets ballot markings correctly and accurately." Ex. 1 at 8. But meaningful review includes access to all of the software components contemplated by the statute.

43. As Dr. Halderman's affidavit explained, it would make "little sense" for the Wisconsin legislature to have authorized the right to access all of the software components contemplated by the statute if it intended to bar candidates from undertaking any security review at all:

> [I]nterpreting Section 5.905(4) to provide access only to the extent necessary to determine whether a given voting machine is capable of accurately tallying ballots in an election, absent external interference or other security concerns, would make little sense. The most effective way to determine whether a voting system can correctly tabulate votes in the absence of manipulation or interference would simply be to feed ballots into the machine and test whether the system interprets and tabulates them correctly, consistent with voter intent. In

[6] *See* Wis. Stat. § 5.905(2) ("Unless authorized under this section, the commission shall withhold access to those software components from any person who requests access under" Wisconsin's open records law).

> contrast, I cannot readily envision a *less* efficient and effective way of determining whether a software component can count and add in the absence of manipulation or interference than reviewing the entirety of the system's software source code. It is difficult to imagine that the Wisconsin Legislature—which expressly provided for candidates in a recount to receive access to "vote-counting source code, table structures, modules, program narratives and other human-readable computer instructions used to count votes with an electronic voting system," Wis. Stat. § 5.905(1)—intended this access to be used only for the extremely limited purpose of assessing whether the machines are programmed to count and add correctly in the absence of any manipulation or interference. Accessing millions of lines of software code for that purpose would be absurd. (Ex. 17, ¶ 12.)

44. Thus, in interpreting the statute to bar any security analysis of the voting systems, the Elections Commission contravened the well settled principle that "statutes should not be construed or interpreted to achieve absurd or unreasonable results." *State v. Yellow Freight Sys., Inc.*, 101 Wis. 2d 142, 153 (1981).

45. In addition to being absent from the statutory text, the Elections Commission's gloss of § 5.905(4) is also inconsistent with the legislative history. The original 2005 bill that ultimately became § 5.905 would have provided that "[t]he coding for the software that is used to operate the system on election day and to tally the votes cast is publicly accessible and may be used to independently verify the accuracy and reliability of the operating and tallying procedures to be employed at any election." Ex. 21 (July 12, 2005 Drafting Notes), at 3. In response to this proposal, the State Elections Board issued a technical memorandum expressing concerns that requiring complete public access is unworkable because there is no "vendor of voting equipment willing to make its source code available for public inspection." Ex. 22 (August 31, 2005 Technical Memo), at 2. In place of the broad public access provision, the Board proposed that the legislature amend the bill to provide that proprietary software would not be publicly

available, but instead permit an "independent review of the source code" by candidates in the event of a recount. *Id.* In other words, the version of § 5.905(4) that was ultimately enacted was intended to serve the original bill's purpose of allowing for "independent[] verif[ication of] the accuracy and reliability of the operating and tallying procedures to be employed at any election," while limiting the universe of persons entitled to carry out such a verification to candidates involved in a recount and their designees. Because the Commission "must presume that the legislature intends for a statute to be interpreted in a manner that advances the purposes of the statute," *Verdoljak v. Mosinee Paper Corp.*, 200 Wis. 2d 624, 635 (1996), any interpretation that would bar Dr. Stein's designees from carrying out such an analysis must be rejected.

46. As the unrebutted expert testimony in the record demonstrates, for software access to meaningfully permit a candidate to verify the systems being analyzed, the access must be sufficient for the candidate's designee to review the four million lines of code from 11 different voting machines and must include an opportunity to determine whether the system that recorded and tallied the votes was exposed or vulnerable to external manipulation by hostile actors.

47. Access must therefore permit examination of the security of the voting systems at issue. Ex. 17 ¶¶ 11-13; Ex. 18 ¶¶ 5, 10. As both Dr. Halderman and Dr. Appel explained, a candidate cannot verify the accuracy of the vote without also reviewing the security of the systems used to record and tally that vote. Confirmation that a system could accurately count votes <u>if not interfered with</u> is meaningless if that system effectively provides an open door to malevolent actors seeking to corrupt the tally. The potential exists for software to be programmed to operate correctly in the absence of any external manipulation or interference yet report incorrect results if a component of the system has been compromised. This potential has

been established in security reviews of voting systems in the past. For example, an attacker might trigger unintended functionality, modify the behavior of the code, or corrupt data about recorded votes—any of which might affect the accuracy of the final tally, even if the system were otherwise correctly programmed to count votes in the absence of such a manipulation. As is well known at this point, there are cybersecurity threats aimed at our election systems. Access to software without the ability to search for such security vulnerabilities is wholly meaningless.

48. Moreover, the Election's Commission decision to "specifically den[y] the campaign's request to implement hypothesis generation and hypothesis testing" is unclear and is capable of unreasonable interpretations. To the extent this language may be read to bar Petitioner's designees from entering the review with any objectives in mind or from formulating plans for the software review in advance based on educated conjecture about avenues of analysis likely to be fruitful, the prohibition on hypothesis generation and testing would be absurd and unworkable.

49. Because the statute nowhere permits the Elections Commission to impose limitations on the particular methods a candidate may use in analyzing software, nor to restrict the purposes for which such a review may be undertaken, the Elections Commission erroneously interpreted Wis. Stat. § 5.905(4) in purporting to impose such limitations. Because a correct interpretation of the statute compels the granting of access to all "software components that were used to record and tally the votes in the election," without restrictions on purpose or methodology, the Elections Commission's decision must be modified pursuant to Wis. Stat. § 227.57(5) to eliminate these restrictions.

50. Likewise, because the Elections Commission's purported imposition of restrictions on the purposes and methodology Petitioner may undertake in conducting the

software review exceeded its authority under the statute, the agency's exercise of discretion was outside the range of discretion delegated to it by law and must be reversed pursuant to Wis. Stat. § 227.57(8).

The Elections Commission's Rejection of Petitioner's Original Plan Was Erroneous

51. Finally, the Elections Commission's rejection of Dr. Stein's original plan for conducting the statutory software review was arbitrary and exceeded its authority.

52. Reviewing over four million lines of code from 11 voting systems takes time. Professor Halderman, a Professor of Computer Science and Engineering and the Director of the Center for Computer Security and Society at the University of Michigan in Ann Arbor, Michigan, prepared Dr. Stein's Plans. His affidavit explains that industry standard holds that scientists can review, at most, 500 lines of code per hour, which would translate to 200 person-weeks of review for the over four million lines at issue here. Ex. 17 ¶ 7.

53. Dr. Andrew Appel, a Professor of Computer Science at Princeton University concurs: his affidavit explains that he reviewed one voting machine for a court case in New Jersey. For that single machine, which had just 130,000 lines of code, his team expended 50 person-weeks. Because 11 machines (and 30 times more lines of code) are at issue here, Dr. Appel believes that a meaningful review in Wisconsin would require 550 person-weeks. Ex. 18 ¶¶ 8, 11.

54. The Elections Commission's rejection of Petitioner's original Plan, and its decision to approve only the more limited Alternative Plan, were based on findings of fact unsupported by substantial evidence in the record. Accordingly, these decisions must be set aside pursuant to Wis. Stat. § 227.57(6).

55. Because the statute nowhere permits the Elections Commission to limit the time or personnel a candidate may use in analyzing software, the Elections Commission erroneously interpreted Wis. Stat. § 5.905(4) in concluding that the original plan was "more expansive than the statute contemplated," Ex. 1 at 7. Because a correct interpretation of the statute compels the granting of access to all "software components that were used to record and tally the votes in the election," the Elections Commission's decision must be modified pursuant to Wis. Stat. § 227.57(5) to permit Petitioner to carry out the original February 15, 2018 Plan.

56. Because the Elections Commission's rejection of the original Plan exceeded its authority under the statute, the agency's exercise of discretion was outside the range of discretion delegated to it by law and must be reversed pursuant to Wis. Stat. § 227.57(8).

PETITION FOR JUDICIAL REVIEW PURSUANT TO WIS. STAT. CH. 227

57. Petitioner repeats and realleges the foregoing paragraphs as if set forth fully herein.

58. Petitioner has an interest in the Elections Commission's March 15, 2018 decision given her clear legal right under Wis. Stat. § 5.905(4) to "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" for President that occurred on November 8, 2016.

59. The March 15, 2018 Decision provides that it is a final decision for purposes of review under Wis. Stat. § 227.53.

60. Petitioner is aggrieved by the Elections Commission's March 15, 2018 decision because it fails to permit Petitioner and her designees to access certain categories of software that indisputably were "used to record and tally the votes in the election," unlawfully purports to restrict the methodologies of analysis Petitioner's designees may perform with respect to the code, and unjustifiably restricts the amount of time her designees may spend reviewing the code.

61. Petitioner has no adequate remedy at law.

PETITION FOR CERTIORARI REVIEW

62. The foregoing paragraphs are incorporated as though fully set forth herein.

63. In the alternative, Petitioner seeks certiorari review available to her pursuant to Wisconsin law.

WHEREFORE, Petitioner respectfully requests the following:

A. That the Court order the Defendant, Wisconsin Elections Commission, to assemble and file with the Court the record of proceedings regarding Petitioner's request for access to software;

B. That the Court conduct a review of the record and determine the following:

i. Because EMS code is used to record and tally votes, the Elections Commission erroneously interpreted Wis. Stat. § 5.905(4) in failing to grant Dr. Stein's designees access to EMS code, in addition to the code Pro V&V already identified. Because a correct interpretation of the statute compels the granting of access to all "software components that were used to record and tally the votes in the election," the Elections Commission's decision must be modified pursuant to Wis. Stat. § 227.57(5) to permit access to all such software.

ii. Because the statute nowhere permits the Elections Commission to impose limitations on the methods a candidate may use when it is granted access to the software, nor restrict the purposes for which such a review may be undertaken, the Elections Commission erroneously interpreted Wis. Stat. § 5.905(4) in purporting to impose such limitations. Because a correct

interpretation of the statute compels the granting of access to all "software components that were used to record and tally the votes in the election," without restrictions on purpose or methodology, the Elections Commission's decision must be modified pursuant to Wis. Stat. § 227.57(5) to eliminate these restrictions.

iii. Because the Elections Commission's imposition of restrictions on the purposes and methodology Petitioner may undertake in conducting the software review exceeded its authority under the statute, the agency's exercise of discretion was outside the range of discretion delegated to it by law, and must be reversed pursuant to Wis. Stat. § 227.57(8).

iv. The Elections Commission's rejection of Petitioner's original Plan, and its decision to approve only the more limited Alternative Plan, were based on findings of fact unsupported by substantial evidence in the record. Accordingly, these decisions must be set aside pursuant to Wis. Stat. § 227.57(6).

v. Because the statute nowhere permits the Elections Commission to limit the time or personnel a candidate may use in analyzing software, the Elections Commission erroneously interpreted Wis. Stat. § 5.905(4) in concluding that the original plan was "more expansive than the statute contemplated," Ex. 1 at 7. Because a correct interpretation of the statute compels the granting of access to all "software components that were used to record and tally the votes in the election," the Elections Commission's decision must be

modified pursuant to Wis. Stat. § 227.57(5) to permit Petitioner to carry out the original February 15, 2018 Plan.

vi. Because the Elections Commission's rejection of the original Plan exceeded its authority under the statute, the agency's exercise of discretion was outside the range of discretion delegated to it by law, and must be reversed pursuant to Wis. Stat. § 227.57(8).

C. That the Court grant such other and further relief as the Court may deem just and proper.

Dated this 16th day of April, 2018.

ATTORNEYS FOR PETITIONER, JILL STEIN

By: *Electronically signed by Christopher M. Meuler*

Christopher M. Meuler (SBN: 1037971)
DAVIS & KUELTHAU, s.c
111 East Kilbourn Avenue, Suite 1400
Milwaukee, WI 53202
414-276-0200
cmeuler@dkattorneys.com

Matthew D. Brinckerhoff*
Debra L. Greenberger*
David A. Lebowitz*
EMERY CELLI BRINCKERHOFF & ABADY, LLP
600 Fifth Avenue, 10th Floor
New York, NY 10020

**Applications for pro hac vice admission forthcoming*