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

INTERIM ADMINISTRATOR MEAGAN WOLFE

COMMISSIONERS

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

Before the Wisconsin Elections Commission

In the Matter of:	)	
Jill Stein Campaign Request for Access to Software Components Pursuant to Wis. Stat. § 5.905	)	**Final Commission Decision**

INTRODUCTION

This matter comes before the Wisconsin Elections Commission ("Commission") for final decision on a request for access to software components filed pursuant to Wis. Stat. § 5.905(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." Wis. Stat. § 5.905(4).

The Commission received a request from a valid party to the 2016 General Election recount, the Jill Stein Campaign for President ("campaign"). Since the request was received, the Commission has worked with the campaign and the two major voting equipment vendors ("vendors") in this State (Election Systems & Software, Inc. and Dominion Voting Systems, Inc.) to devise a plan which grants access to software components used to record and tally votes cast that is reasonable, meaningful and consistent with both the letter of the statute and the statute's intent.

The commission has previously made unanimous decisions on several aspects of the campaign's request. This decision incorporates those actions and resolves issues related to software component access after consideration of the competing review plans submitted by the vendors and the campaign.

The associated documents and software components identified by an accredited Voting Systems Testing Lab (VSTL) are incorporated here, are part of the full administrative record for this matter and are addressed in subsequent narrative sections of this final decision.

Upon consideration of the written materials and oral testimony provided to the Commission, a final decision in this matter is issued herein.

I. GENERAL BACKGROUND

A. Electronic Voting Systems in Wisconsin

Wisconsin law requires a voting system to be certified before use in an election. All electronic voting systems used in Wisconsin during the 2016 General Election had been certified on both the federal and state level. Federal testing is coordinated by the Election Assistance Commission (EAC) and voting systems are tested to the standards outlined in the 2005 Voluntary Voting System Guidelines (2005 VVSG). The testing prescribed by the 2005 VVSG includes source code review, verification of system components and functional testing that includes a security assessment. The 2005 VVSG outlines the objectives of the security standards for voting systems as:

- Protect critical elements of the voting system
- Establish and maintain controls to minimize errors
- Protect the system from intentional manipulation, fraud and malicious mischief
- Identify fraudulent or erroneous changes to the voting system
- Protect secrecy of the voting process

Systems certified for use in Wisconsin before the adoption of the 2005 VVSG were tested to the previous iteration of those standards, which also include security testing of the system. In addition to these certification requirements, all systems approved for use in Wisconsin must be paper ballot-based or produce a Voter Verified Paper Audit Trail (VVPAT) that allows a voter to confirm their selections before casting a ballot.

There were eleven different voting systems in use in Wisconsin during the 2016 General Election. Three of these systems include Direct Recording Electronic (DRE) touchscreen voting machines that record and tally votes, while the other eight systems include optical scan tabulators. Optical scan tabulators read votes marked on paper ballots as they are inserted in the machines to produce election results. All voting equipment used in this election was required to be publicly tested no sooner than ten days before Election Day. The purpose of the public test is to confirm the accuracy of the election programming and to ensure the voting equipment is functioning properly before being used in the election.

B. 2016 General Election

For the 2016 General Election in Wisconsin, 2,976,150 total votes were cast for the Office of President, with 2,447,462 ballots processed by optical scan tabulators and 299,503 votes cast on DRE touchscreen voting machines. The Wisconsin Elections Commission (WEC) did not receive any reports of voting system failure during the 2016 General Election that would indicate any voting machines were compromised in a manner that would prevent them from accurately recording and tallying votes.

C. 2016 General Election Recount

In addition to the original canvassing of votes after the 2016 General Election, election results in Wisconsin were subject to a statewide recount for the Office of the President. Recount law in Wisconsin identifies the county board of canvassers as the body responsible for conducting a recount for a

statewide office and Wis. Stat. §5.90(1) permits the county board of canvassers to employ voting machines to recount the ballots. The county board of canvassers can also decide to hand count all ballots cast for the office subject to recount. During the recount, WEC records indicate roughly 58 percent of all ballots were counted by hand with the remaining percentage processed with the assistance of optical scan tabulators.

The recount began on December 1, 2016 and the recount results were certified by the WEC twelve days later. Counties that chose to employ voting machines to conduct the recount did so with reprogrammed memory devices that mirrored the original Election Day programming. Several counties rented high-volume optical scan tabulators that allowed them to process ballots at a higher rate than the optical scan tabulators regularly used at the polling place level.

The results of the recount did not identify any systematic failure or tampering with voting equipment during the 2016 General Election. The recount process did identify a number of election official errors that are represented in the difference between the original canvass results and the recount results. Some of these errors include incorrectly rejected absentee ballots and votes for registered write-in candidates that were not tallied in accordance with the law. Ultimately, the certified results following the recount changed very little from the original results – with Donald Trump gaining 844 votes, Hillary Clinton gaining 713 votes for a net gain of 131 votes for Donald Trump out of almost 3 million votes cast.

D. Post-Election Audit – 2016 General Election

In addition to the statewide recount for the Office of President, the WEC was also required to administer a post-election voting equipment audit after the 2016 General Election. Participants in the audit are selected at random and the sample selected is designed to include a representative amount of each type of voting equipment used during the General Election. The audit was originally postponed until after the conclusion of the recount and was ultimately limited to municipalities who used optical scan voting equipment during the recount. In total, thirty-two reporting units originally selected to conduct post-election voting equipment audits were determined to be subject to audit. The results of the audit indicate both the accessible voting equipment and tabulation equipment used and audited for the 2016 General Election recorded and tabulated votes as expected and according to certification standards. The audit results indicated there were no identifiable bugs, errors, or failures of the tabulation voting equipment, and that discrepancies identified during the audit were the result of human error when conducting the audit.

E. Commission Confidence in Performance of Electronic Voting Systems for 2016 General Election

The combination of evidence outlined above supports the Commission's belief that voting equipment accurately recorded and tallied votes in Wisconsin during the 2016 General Election. Voting systems used during this election were certified on both the federal and state level and the programming for these machines was verified during required pre-election public testing. In addition, several post-election procedures also served to verify both the performance of the voting systems and the actual outcome of the election for the Office of President. The significant number of ballots that were hand-counted during the statewide recount would have identified election results that were altered as a result of voting machine malfunction or tampering. The recount results either did not identify any discrepancies with

the original election results or identified issues that were the result of local election official error and not attributed to the inability of the voting equipment to accurately record and tally votes. The post-election voting equipment audit added a final verification that election results produced by voting machines were accurate.

F. Campaign's Request for Access

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 email 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.

Since the request was received, Commission staff had conversations with both representatives of the campaign and representatives of the vendors to collect information regarding which software components the parties believed were subject to review under the statute, what sort of non-disclosure agreement should be signed prior to access being granted, and what additional parameters should be in place to facilitate a review that is reasonable and meaningful. In reaching its decision, the Commission has considered all of the submissions made by the campaign and the vendors in this matter.

II. DISCUSSION

A. Access to Software Components Per Wis. Stat. § 5.905

Regardless of whether the Commission is confident the electronic voting systems produced accurate results for the 2016 General Election, Wis. Stat. § 5.905 contains mandatory language requiring that access to software components be provided if certain conditions are met. The Commission "shall grant access" to the software components that were used to record and tally votes. Wis. Stat. § 5.905(4). The access is limited to parties of a recount and only if the parties or individuals designated by the parties enter into an agreement which obligates him or her to exercise the highest degree of reasonable care to maintain the confidentiality of all proprietary information to which the person is provided access.

Determining what access to software components is permitted under Wis. Stat. § 5.905 is an issue of first impression for the Commission. The Commission is not aware of any similar statutory provisions in other states that grant such unprecedented access to proprietary software used in electronic voting equipment.

Wis. Stat. § 5.905 states in its entirety:

> **5.905 Software components.**
> **(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).

The software components contained in the electronic voting systems are part of the vendors' intellectual property and are the product of significant research and development. The software components which record and tally votes in this state are considered confidential and proprietary, and the Commission is responsible for maintaining that confidentiality. Wis. Stat. § 5.905(2). The Commission must balance this responsibility with the campaign's right to reasonable and meaningful access under the statute.

B. Software Components Subject to Review

Wis. Stat. § 5.905(2) tasks the Commission with determining 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. The Commission retained the professional services of Pro V & V, Inc. ("Pro V & V") a U.S. Election Assistance Commission accredited Voting System Testing Laboratory (VSTL) to assist the Commission in making this determination.

Pro V & V obtained a copy of the source code which had been escrowed by the vendors for each of the electronic voting systems used in the 2016 General Election. Pro V & V reviewed the code versions for

each of the systems used and made determinations as to which pieces of the code "recorded and tallied" votes. Pro V & V provided the Commission with a report, detailing the work that was completed and the results. Along with the report, Pro V & V provided the Commission with "packages" of software code for each of the systems and code versions that were reviewed. The "packages" isolated from the full source code contain only the components that Pro V & V believed were available for access under Wis. Stat. § 5.905. A copy of the report issued by Pro V and V (Version 2), was adopted by the Commission at its March 2, 2018 meeting, and is included with this final decision at Attachment 1. The "packages" are in possession of the Commission and available when the review occurs.

Only software components and associated code versions that were in use for the 2016 General Election are subject to review. A final list of the code available for review was approved by the Commission at its March 2, 2018 meeting, and is included with this final decision at Attachment 2.

C. Confidentiality and Nondisclosure Agreement

Wis. Stat. § 5.905(4) tasks the Commission with ensuring that before access to software components is granted, that the individual granted access "enters into an 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…"

The Commission approved a Confidentiality and Nondisclosure Agreement ("agreement") that individuals, identified by the campaign as being authorized to receive access, must execute and provide to the Commission before access to the software components is granted. The agreement was approved by the Commission at its January 31, 2018 meeting, and is included with this final decision at Attachment 3.

D. General Software Components Review Parameters

At the Commission's January 31, 2018 meeting, the Commission approved a memorandum containing general parameters for the review of software components under Wis. Stat. § 5.905. These general parameters were required to provide groundwork to ensure that any review of software components would be done securely and that the vendors' proprietary information would be protected during the review.

As part of these basic parameters, the Commission asked the campaign to provide a review plan that would clearly set out how it envisioned the review would be conducted, including time needed, number of individuals that would be necessary to conduct the review and/or proposed methods.

The parameters were approved by the Commission at its January 31, 2018 meeting. The Commission's action, including changes made by the Commission from the original staff recommendations, are reflected in the memorandum which is included with this final decision at Attachment 4.

E. Software Components Review Plan

The campaign and the vendors strongly disagree regarding the scope of the review required and authorized by Wis. Stat. §5.9095. On February 15, 2018, the campaign submitted to the Commission its "Stein Campaign Review Plan." The plan proposed an election software component testing methodology called Open Ended Vulnerability Testing (OEVT), which involves multiple rounds of vulnerability hypothesis generation, refinement and testing, based on a combination of research and code review. The plan proposed a three-phase process comprised of on-site code review, hypothesis generation and hypothesis testing, requiring an investment of 145 person-weeks and which would occur over a period of two and one-half months.

The vendors submitted correspondence objecting to the campaign's plan on February 26, 2018. The Commission met on March 2, 2018 to discuss the parties' submissions. The Commission provided an opportunity for counsel representing the campaign and the vendors to present their arguments and answer Commissioners' questions. The Commission rejected the campaign's request to adopt its plan and direct its implementation. The Commission advised the campaign that it viewed the plan as more expansive than the statute contemplated, and requested that both parties submit proposed plans for the Commission's further consideration.

The campaign and the vendors submitted revised proposals on March 9, 2018. The Commission met again on March 13, 2018 to consider the proposed plans. Counsel for the campaign and the vendors again addressed the Commission and answered its questions in open session. The Commission then convened in closed session to discuss the proposed plans and directed staff to draft a proposed decision as outlined below.

The campaign's "Alternative Plan" significantly reduced the requested amount of time involved and the scope of its proposed review compared to its original plan, but continued to propose use of the Open Ended Vulnerability Testing methodology. The campaign asserted that the accuracy of the voting equipment in tallying and recording votes cannot be assessed without also evaluating the security of the voting system software, and that OEVT facilitates the discovery of flaws in voting system software architecture, design and implementation which can be exploited to change the outcome of an election. The campaign Alternative Plan proposed an examination period covering 33 days, consisting of three separate periods of on-site code review and testing separated by two periods of hypothesis generation.

The vendors' "Exemplary Review Plan" asserted that the campaign's proposed OEVT analysis exceeds the scope of the software component access permitted by Wis. Stat. § 5.905. The vendors' recommended plan proposed black box testing using test ballots to observe how the voting equipment tabulators tally and record votes using the software components, similar to the process used by Commission staff as part of its voting equipment certification testing as well as that used by municipalities when conducting pre-election logic and accuracy tests. The vendors' plan proposed that the campaign be allowed to inspect the voting equipment tabulator audit logs to verify the integrity of the system's preparation, operation and output. The vendors' proposed plan does not include actual viewing of the software source code or interaction with the software using automated code analysis tools or penetration testing, or any type of hypothesis generation and testing.

After considering the submissions of the parties and their arguments and following the Commission's deliberations regarding the intent of Wis. Stat. § 5.905 and the scope of review authorized by that statute, the Commission has determined that neither plan adequately describes the access to the software components which must be provided to the campaign. In short, the Commission has determined that the campaign's proposed plan and its use of OEVT to assess the security and potential vulnerabilities of the voting equipment significantly exceeds the access described by the statute. At the same time, the Commission has determined that the vendors' proposed plan fails to allow an opportunity to actually review the software and assess whether any potential flaws exist in the source coding related to the accuracy of the vote tally and recording.

III. FINDINGS OF FACT AND CONCLUSIONS OF LAW

Based on the process and factors described above, the Commission makes the following findings and orders related to the review plan:

A. The National Institutes of Standards and Technology ("NIST") defines OEVT as follows:

> **1.2 Definition of OEVT:** Vulnerability testing is an attempt to bypass or break the security of a system or a device. Like functional testing, vulnerability testing can falsify a general assertion (namely, that the system or device is secure) but it cannot verify the security (show that the system or device is secure in all cases). Vulnerability testing is also referred to as penetration testing. Vulnerability testing can be performed using a test suite or it can be open-ended. Open ended vulnerability testing involves the testing of a system or device using the experience and expertise of the tester; using the knowledge of system or device design and implementation; using the publicly available knowledge base of vulnerabilities in the system or device; using the publicly available knowledge base of vulnerabilities in similar system or device; using the publicly available knowledge base of vulnerabilities in similar and related technologies; and using the publicly available knowledge base of vulnerabilities generally found in hardware and software (e.g., buffer overflow, memory leaks, etc.)[1]

B. Use 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 Wis. Stat. § 5.905. The purpose of the statute is to provide parties to a recount the opportunity to review the accuracy of the voting equipment's vote-tallying software, and to determine whether the tabulator interprets ballot markings correctly and accurately. The OEVT methodology is focused on security and penetration testing, and determining whether any vulnerabilities exist that could potentially be exploited to alter results after they are tabulated correctly, not on verifying the accuracy of the code that records and tallies the votes.

[1] 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 Commission finds that, while the OEVT methodology was developed by the National Institute of Standards and Technology ("NIST"), it has not been formally adopted into the NIST standards related to accuracy testing because its purpose is penetration and security testing. The Commission considered the use of OEVT methodology as used in the review of voting equipment in the states of California and Ohio, and finds that Wis. Stat. § 5.905 does not permit or contemplate a similar "end to end" or "top to bottom" review or access. The statute simply provides access to software components and does not mention the use of penetration testing to determine or verify accuracy, or the ability of a recount party to interact with or test the code to find hypothetical security flaws. Potential or hypothetical flaws related to security that may or may not be discovered in escrowed software components have no bearing on whether the voting equipment accurately recorded and tallied votes cast in November 2016.

D. The Commission finds that the vendors' proposed plan partially satisfies the intent of Wis. Stat. § 5.905, because the accuracy of the software components which tally and record the votes can be evaluated only by observing the results of how the software interacts with the voting equipment hardware and actual test ballots. The Commission concludes that the process outlined in the vendors' Exemplary Review Plan shall be incorporated into the access provided to the campaign pursuant to Wis. Stat. § 5.905. Based on representations made by counsel for the vendors at the Commission's meeting of March 13, 2018, the campaign shall be allowed the opportunity to mark the test deck instead of the vendors. As outlined in the vendors' proposed plan, the campaign shall have access to the audit logs which otherwise are not made available to the public during other testing of the equipment by the Commission. The vendors' proposed plan also identified 100 test ballots as the standard to be used for testing each piece of equipment. If the campaign deems this number of test ballots to be insufficient, the Commission reserves the right to alter the number of required tests ballots per piece of voting equipment.

E. The Commission further finds that the vendors' proposed plan does not fully satisfy the requirements of Wis. Stat. § 5.905, which mandates access to the actual software components' source code for whatever value that access has in evaluating the accuracy of the software components. In order to ensure that "access" to the software components has some meaning, the Commission finds that the statute contemplates some physical access to and review of the code, and not simply a repeat of the same process utilized for testing and certification of the voting equipment, which is essentially the process proposed by the vendors (except for access to the audit logs). While observation of the results of ballot tabulation by the voting equipment can demonstrate the accuracy of the software components, the Commission concludes that the statute contemplates more, regardless of whether providing access to the source code is the ideal method to verify accuracy of the equipment used. The Commission cannot nullify the meaning of the term "access" in the statute by denying the campaign an opportunity to manually review the software components' source code and use automated code analysis to evaluate its accuracy in tallying and recording votes.

F. In addition to the process described in paragraph III. D. above, the Commission directs that portions of the "Code Review" provisions of the campaign's Alternative Plan shall be incorporated into the process for providing access to the software components. Specifically, the campaign's representatives may perform manual source code review and may also use automated

code analysis tools to analyze the source code for buffer overflows, memory leaks, dead code, and otherwise suspicious code.

G. The campaign's source code review shall be performed using "read only" access and the campaign shall not interact with or perform testing of the software components. The campaign shall be provided with access to view the source code on the screen with the assistance of pre-approved tools to read the code, so the campaign can determine how the code tallies and records votes and whether it does so accurately. The Commission specifically denies the campaign's request to implement hypothesis generation and hypothesis testing as outlined in its Alternative Plan.

H. The Commission directs that the two components of the process for providing access to the software components – the source code review and the processing of test decks – shall be completed over a time period equivalent to that outlined in the campaign's Alternative Plan – 12 people for a 3-week period (36 person-weeks). However, due to the administration of the Spring Election on April 3, 2018, any on site activities related to the campaign's access shall commence no sooner than April 9, 2018. The on-site review of source code and observation of the test deck results shall be completed within a period of 33 days. The specific dates scheduled for completion of the process shall be determined by Commission staff after consultation with the campaign and the vendors.

I. The campaign and the vendors are each responsible for bearing their own costs in executing the review plan. Representatives of the vendors may observe the campaign's review of source code and test ballot process, and Commission staff is authorized to resolve or decide any issues or disputes related to the campaign's access. The Commission shall provide a secure location for the review process and storage of any equipment used for the duration of the review.

This final decision and attachments constitute the Commission's decision on the campaign's request for access to software components pursuant to Wis. Stat. § 5.905 for purposes of judicial review. This decision is final for purposes of judicial review of agency administrative decisions pursuant to the provision of Wis. Stat. § 227.53.

This decision was approved by a 6-0 vote of the Wisconsin Elections Commission on March 15, 2018.

Wisconsin Elections Commission

Mark Thomsen, Chair

March 15, 2018
Date

ATTACHMENT A

Test Report

Software Component Review Report for the State of Wisconsin

Prepared by: _____

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.

ATTACHMENT B

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

-2016 General Election-

Unity 3.0.1.0
MIOO 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
MIOO 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

ATTACHMENT C

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

CONFIDENTIALITY AND NONDISCLOSURE AGREEMENT

1. THIS CONFIDENTIALITY AND NONDISCLOSURE AGREEMENT ("Agreement"), dated this ____ day of _____, 20__, by _____ ("Recipient"), obligates the Recipient to exercise the highest degree of reasonable care to maintain the confidentiality of all proprietary information to which the Recipient is granted access, as described in the Final Decision, pursuant to Wis. Stat. § 5.905 (4) and for no other purpose.
2. Recipient agrees to exercise the highest degree of reasonable care to maintain the confidentiality of all proprietary information to which access is provided and not disclose or reveal any proprietary information to any person, pursuant to Wis. Stat. § 5.905 (4).
3. After the Recipient's execution and delivery of this Agreement, and pursuant to the terms of the Final Decision, the Recipient shall be granted access to the software components used to record and tally the votes cast in the November 8, 2016 General Election conducted in the State of Wisconsin pursuant to Wis. Stat. § 5.905 (2).
4. Each Recipient designated under Wis. Stat. § 5.905 (4) shall execute and deliver this agreement to the Wisconsin Elections Commission ("WEC") prior to access being granted.
5. The review of the software components shall take place in accordance with the terms and conditions of the review as determined by the WEC as stated in the Final Decision.
6. Recipient's obligation to exercise the highest degree of reasonable care to maintain the confidentiality of all proprietary information survives this agreement and shall continue permanently.

7. Recipient acknowledges that Recipient is responsible for any unauthorized disclosure and shall pay for any and all damages that relate or arise out of the review of the software components.

By executing this Agreement, I agree to abide by the terms set forth herein.

Recipient:

_____ (Printed Name, Title)

_____ (Address)

_____ (Phone Number)

_____ (Email Address)

_____ (Signature)

_____ (Date of Signing)

Upon Execution of this Agreement:

Send to:
Wisconsin Elections Commission
Attn: Legal Counsel
212 E. Washington Ave., 3rd Floor
P.O. Box 7984
Madison, WI 53707-7984
elections@wisconsin.gov

ATTACHMENT D

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

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 #32: Except for the deadline related to the written examination plan as described in amended Paragraph 4.a. of the memorandum, tThe 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.