STATE OF CALIFORNIA

SECRETARY OF STATE

OFFICE OF VOTING SYSTEMS TECHNOLOGY ASSESSMENT

In the Matter of:	)
	)
PUBLIC HEARING:	)
	)
DOMINION VOTING SYSTEMS	)
	)
IMAGECAST REMOTE 5.2 REMOTE	)
	)
ACCESSIBLE VOTE BY MAIL	)
	)
SYSTEM	)
_____	)

PUBLIC HEARING

Secretary of State Building

1500 11th Street

Sacramento, California

April 27, 2018

9:00 A.M.

Reported by:

Peter Petty

APPEARANCES

STAFF

Susan Lapsley, Administration

NaKesha Robinson, OVSTA

Rodney Rodriguez, OVTSA

Todd Ross, OVTSA

CONRACTORS/CONSULTANTS

Mike Santos, SLI Compliance

PUBLIC COMMENT

Fred Nisen, Disability Rights California

APRIL 27, 2018, 9:03 A.M.

SACRAMENTO, CALIFORNIA

MS. LAPSLEY: All right. Good morning. Well, it's a couple minutes after nine. We'll go ahead and get started. I'd first like to introduce Staff, and then we'll kind of cover the ground rules of this public hearing.

Here on stage, we have Todd Ross, who is a member of the Office of Voting Systems Technology Assessment, OVTSA. I'll let Mike -- we'll hold off on Mike, because you're not a member of OVTSA. You don't count as Staff. NaKesha Robinson, also a member of OVTSA. And down here we have Rodney Rodriguez, also with OVTSA. Rodney will be handling the timing of public comments, as well as speaker cards, and making sure that everything runs smoothly here as far as sound and getting everyone what they need.

Just a few ground rules. There's no food or drink in the auditorium. We will be taking public comment about the following -- about Dominion Voting Systems ImageCast Remote 5.2, Remote Accessible Vote By Mail System. RAVBM is the abbreviation of that.

The Staff Reports, consultant's reports and other tests are available on our website at www.sos.ca.gov/elections/votingsystemsvendors/dominion. For the system being heard, the Staff Report will be given, then the consultant's report. After that the vendor will

have an opportunity to respond, and then it will be open for public comment. All those requesting to speak during the public comment period for the system must complete a speaker request card, which is available -- they are available at the entrance. If you didn't get one and would like one, please raise your hand and let Rodney know and he can run one to you.

Speaking time will be limited to three minutes. The timekeeper will advise when 2 minutes 30 seconds has elapsed, and then again when 3 minutes has elapsed. Rodney wanted to use a big hook today, but we wouldn't let him. So he'll let you know by holding up a notice card. A speaker may use additional time that has been ceded to them by a maximum of two other people who have signed a speaker card request. If you wish to cede your time to another speaker, please that person's name in addition to your own name on your speaker's request card.

We have a small house today, so I won't give my normal comments about people coming a long ways and being respectful. I assume, looking at the faces here, everyone is very respectful, except for may Waldeep up there in the corner, who has his drink in hand.

Please note that the court stenographer is taking a transcription of the meeting today. This means that if you speak, your name and your comments will be part of the

public record. They will be posted on our internet website at some point, so please state your name clearly for the stenographer prior to beginning.

The public hearing is also being videotaped, which will also be part of the public record.

Written public comments on this item can be submitted to Voting Systems at sos.ca.gov, or by U.S. Mail to the Secretary of State's Office, Attention: Voting System Comments, at 1500 11th Street, 6th Floor, Sacramento, California 95814. Any written comments submitted to the Secretary of State, whether they be via email or U.S. Postal, will become, also, part of the record.

With that, we'll go ahead and we will turn it over to NaKesha to give the Staff Report.

MS. ROBINSON: All right. Good morning, everyone. Dominion Voting Systems submitted an application for the ImageCast Remote 5.2 System on September 5th, 2017. ImageCast Remote 5.2 is a vendor-hosted application solely for the purposes of ballot marking, pursuant to Elections Code sections 303.3 and 19283. ImageCast Remote 5.2 was evaluated against the applicable portions of the California Voting Systems Standards, or CVSS.

Upon receipt of a completed application the Secretary of State released a Request for Quote for

assistance with source code review, telecommunications and security review, as well as usability, accessibility and privacy testing.

Through a formal California contracting process the Secretary of State awarded a contract to SLI Compliance, a division of Gaming Laboratories International, LLC, to assist with testing.

Dominion Voting Systems Remote 5.2 Remote Accessible Vote By Mail System application is a web-based interface. The voter can optionally use a screen reader to navigate through the -- through the screens. After marking their cast vote record and reviewing their selection, the voter must print their selections. The printed paper-cast record is returned to the local elections official, where it will be remade into a ballot. The printed paper-cast record and the ballot are kept together for auditing purposes.

Accessibility and functional testing of the system was conducted by SOS staff. The functional test was conducted at the Secretary of State's Office in Sacramento, California during the month of November 2017.

End-user accessibility testing was conducted in three waves. Wave one user accessibility testing was performed by nine volunteers throughout the State of California from November 30th to December 1st, 2017. Wave

two took place from December 4th to December 8th, 2017, concluding with wave three from December 18th to December 22nd, 2017, where we had 29 volunteer testers. The additional testing was conducted by SLI during the month of March 2018.

For the functional test, the Secretary of State's Office provided Dominion with three test ballot data sets of California elections: one, the State of California Primary Election, which was comprised of a fictional jurisdiction; two, a State of California General Election, which was also a fictional jurisdiction; and last, a local jurisdiction fictional ranked choice election.

The system was also exercised for under-votes, over-votes and write-ins. The system successfully warned users of under-votes and over-votes, as well with write-in candidates, it does have a 50 character limit.

During accessibility, usability and privacy testing, again, we conducted three waves. And, also, SLI conducted accessibility, usability and privacy testing.

During the testing with the end-users that were recruited statewide, the testers were asked to complete pre-test and post-test surveys, documenting such information as demographics, the technology that was used for testing, and the testers post-test experience using the system. The survey results of each are included in

Attachment A of the Staff Report. Please note that personal identifying information has been redacted.

During the testing conducted with end-users, there are approximately 15 technical issues that were identified. Each has a response and/or mitigation, which can be found in the Staff Report.

SLI conducted an additional accessibility, usability and privacy test, as well. Phase one of SLI's testing was a review of the ImageCast Remote 5.2 documentation of usability and accessibility performed during system development. Phase two included all accessibility and usability testing. And phase three included privacy testing. Additional details regarding SLI's testing can be found in the Staff Report, as well as during the next presentation, Mike Santos will elaborate a little bit further.

During usability testing, SLI identified one requirement that was not met. That is CVSS 3.2.7.C.2. Review of that requirement showed that navigation keys, up and down arrows, tab did have repetitive effect. Dominion will address that by adjusting their use procedures accordingly.

During accessibility testing by SLI, additional testing was also conducted against the applicable portions of section 508. And during that testing, it was determined

that all requirements were satisfactorily met.

During privacy testing, SLI evaluated ImageCast Remote for compliance with California Elections Code requirements within an RAVBM system, in addition to the applicable portions of the CVSS. During that testing, all requirements were satisfactorily met and/or covered.

And next, during the security and telecommunications testing, SLI conducted a documentation review, functional security testing, and telecommunications and data transmission testing. A summary of each of the applicable standards, as well as whether those standards were met, are covered within the Staff Report.

During the security and telecommunication's testing, SLI did identify two potentially high security vulnerabilities, one being potential cross-sites scripting opportunity and select components of the system. Dominion has provided a vendor mitigation, as well as a response, which can be found within the Staff Report. The second issue, potential sequel injection vulnerabilities arise when user-controllable data is incorporated into database sequel queries in an unsafe manner. And again, Dominion did provide a vendor response, as well as mitigation to that vulnerability.

And then finally, during the software review testing, the purpose of this testing was to review and

identify any discrepancies within the software code and compliance with the California Voting System Standards. During that testing, SLI discovered one discrepancy. There were 180 source code requirements found to be at issue with the RAVBMS source code base reviewed. As a result, 108 discrepancies were written against the code base. Dominion did provide a mitigation in response to that, as well.

And one other item I'd like to go back to, during our end-user testing, one of our test volunteers did identify or make some comments that I did not get a chance to address during the Staff Report, so I'd like to address those now. It is regarding the PIN feature within Dominion's RAVBM system.

So the PIN is a feature that can be turned on and off, just like the capture functionality. Depending upon how the jurisdictions and/or the SOS provides guidance on using those -- issuing PINs. The system also provides options to have a PIN issued via telephone and/or a postcard. And also to be very clear, the RAVBM cast vote record will be remade into a ballot. And while we understand Dominion does have the capability to read those cast vote records directly within their voting system, we must have an official ballot. So all the RAVBM cast vote records will be remade.

And with that, that concludes my presentation of

the Staff Report.

Next up, we'll have Mike Santo from SLI.

MR. SANTOS: Good morning. I am Mike Santos from SLI Compliance. As NaKesha just mentioned, we were tasked with doing source code review, security and vulnerability testing, as well as accessibility, usability and privacy testing.

In terms of source code review, there were approximately 319,000 lines of source code and comments that were subjected to review. Some of the criteria that we were using for the review process was adherence to applicable standards of the CVSS, adherence to other applicable coding format conventions and standards, including best practices for the coding languages being used, analysis of the program logic and branching structure, as well as evaluating whether the system is designed in a way that allows meaningful analysis.

Also, as NaKesha mentioned, during the source code review there were 180 source code discrepancies that were found. They were -- they covered six different requirements.

There were some 80 instances that were noted where lines of source code exceeded more than 120 characters in length, 71 instances that were noted where numbers were not set to a constant, 23 instances that were

noted where variable declarations were without comment, 10 instances were noted where no default case existed, 2 instances were noted where variable names were not differing by more than one character were being utilized, and there was 1 instance noted where inconsistent indentation was implemented. So that was the findings from the functional system source code review.

We also performed a vulnerability review on the source code where we were searching for exposures to commonly-exploited vulnerabilities, evaluating the use and correct implementation of cryptography of key management, evaluating the likelihood of security failures being detected in terms of like audit mechanisms and where the data could be subject to tampering, evaluating the risk that a user can escalate their capabilities beyond those authorized, evaluating the design and implementation to ensure that sound generally-accepted engineering practices are being followed and that the code is being written defensively, evaluating for embedded exploitable code that could be triggered to effect the system.

We evaluated the code for dynamic memory access features which would permit the replacement of certified executable code or control data or insertion of exploitable code or data. And we also were evaluating the code for use of runtime scripts, instructions or other control data that

can affect the operation of security-relative functions or the integrity of the data itself.

So upon looking through those 319,000 lines of code for those criteria, no vulnerabilities were found within the system. And as a result, no findings were written against the code base with regards to vulnerability.

We were also tasked with a security review. We looked at various aspects of security, including general access control, access control identification, access control authorization, and general access control.

Let’s see here, in terms of general access control, we were looking for authentication that included methods for both the voter-facing application, as well as the administrative application. The security -- the general access control security was tested on the architecture pieces, client application, administrative application, which were accessible remotely.

In terms of access control identification, the system was determined to use a client server system to authenticate registered users and serve up the correct ballot for a particular voter using pre-defined ballot rules and voters that can be imported by the jurisdiction. Role-based access controls were determined to be in place for administrative login purposes.

With regards to access control authorization, all administrative access is controlled by username, password combinations, and there is a role-based administrative access in place. Also, the ability to assign voters to different electoral groups or electoral districts, it gives the ability to assign ballots to voters in accordance with specific CVSS rules.

For access control analysis, we attempted XSX (phonetic) attacks, sequel injection attacks, direct re-listings, and scans attempting to pull directory file lists scanned for default, http login pages. We scanned for robot text files and pulled SSL certification information. We performed a full vulnerability scan, as well.

Sorry.

For telecommunications and data transmission, the system utilizes electrical transmissions, and the ballot is sent by SSL. No receipt is utilized to verify the transmission. The client generates a blank ballot which does not contain voting selections, so once the ballot is delivered and until the ballot package is saved there are no external communications between the voter and the ballot delivery system. All interactions remain local to the voter’s environment.

In terms of security vulnerabilities, we were tasked with determining, A, if there were security

vulnerabilities, and B, if there were, to try to indicate the level of exploitation that the vulnerability would require access by.

And those are broken down into four different categories: a voter, who usually has low knowledge of the voting machine and design and configuration; a poll worker, who usually also has a low knowledge of the voting design and configuration, but has more access to anything, which in the case of an RAVBM system (indiscernible) going to have poll workers; election official insiders who have a wide range of knowledge of the voting design and configuration and may have unrestricted access to the machine for long periods of time; as well as a fourth category of a vendor insider that has great knowledge of the voting machine design and configuration and have unlimited access to the machine before it's delivered to the purchaser, and thereafter may have unrestricted access with performing warranty and maintenance service, and when providing election administrative services.

The ability to tamper with the client site application is always present due to the fact that there are no server site verifications or validations in place after the ballot has been generated. So at that point, you know, somebody can sit there for days on end and do whatever they want to that ballot. In this context,

however, the ability to effect large numbers of ballots is reliant upon server site compromise, which may also include distributed denial (phonetic) of service attacks.

The voter is given the ability to proof and confirm ballot selections within the system, as well as the printed paper ballot, so there is a final confirmation screen with the system. And then once you've printed your paper ballot, you have that ability to do a final check of that ballot prior to submitting it or being cast.

Security testing of the server site hosting security included application scanning and vulnerability scanning. The results of the scanning revealed potential vulnerabilities that is estimated would have a minimal impact on the overall security of the application being tested. And those were basically what NaKesha mentioned a few minutes ago and, I guess, is in the final reports on the website.

The third area that we were tasked with reviewing was the usability and accessibility testing, as well as privacy testing.

In terms of usability and accessibility testing, some of the items that we were looking at were that the system allows the voter, at the voter's choice -- it's kind the basics of voting the ballot, that the system would allow the voter, at the voter's choice, to submit an under-

voted ballot without correction. That would provide the voter the opportunity to correct the ballot for an under-vote before the ballot is cast and counted.

It would prevent voters from selecting more than the allowable number of choices for each contest, so it doesn't allow over-voting.

It provides feedback to the voter before final casting of the ballot that identifies specific contests for which the voter has selected fewer than the allowable number of choices, providing the voter the opportunity to correct the ballot.

It allows the voter to change a vote within a contest before advancing to the next contest, to provide navigation controls that allow the voter to advance to the next contest or go back to the previous contest before completing the vote on the contests currently being presented. So it's really just checking, you know, a lot of the -- some of the basic rules, the no over-voting, letting you know if you've under-voted, and allowing you to vote, basically, any contest in any manner in any order that that voter prefers. A voter was able to vote appropriate contests in any manner or order they wished and was notified when under-voting, and was prevented from over-voting.

We were also looking at cognitive issues,

completeness of instructions, availability of assistance from the system, plain language being used, context before actions, no bias among choices, ballot design, conventional use of colors, icons and languages, as well as perceptual issues, including accommodation for color blindness and no reliance solely on color so that color coding is not used as the sole means of conveying information.

Interaction issues, we were looking at no page scrolling being allowed, unambiguous feedback for voter's selection, so that was very obvious that what they were selecting as their choice. We looked for accidental activation, size and separation of touch areas, repeating keys, timing issues, initial system response times, maximum completed response time for vote confirmation, maximum completed system response time for all operations, and voter inactivity time.

As NaKesha mentioned, we did see an issue with the no repeating keys, that key presses were allowed to be repeated. And it sounds like Dominion Voting Systems has implemented a mitigation for that.

In terms -- we were also looking at alternative languages, general support for alternative languages, complete information in an alternative language, auditability of records for English readers, and voter control of language. An issue that was seen in terms of

voter control with the language that the system allows the voter to select among the available languages throughout the voting session, while preserving the current votes.

So once a voter selects a language and they download that ballot, the connection to the server is broken and that ballot is local only to that device that the voter is voting on. So should they decide to change languages, they would need to go back and access a whole new ballot and it would not carry over anything that they had voted in the first language to a second language, so that was one thing that was noted.

There were a number of requirements that were related to hardware in the voting environment where the voter would be casting their ballot that were deemed not applicable as the voter will be utilizing their own equipment, so we really couldn't speak to hardware-oriented items.

In terms or privacy, some of the categories were visual privacy, auditory privacy, and no receipts. And again, this was as a Remote Access Vote-By-Mail System. The voting will occur in an environment of the voter's choosing. And all privacy issues will be reliant upon where they choose to cast their -- or to mark their ballots.

Some final requirements that were looked at were

related to, I think this is Rule 19295, RAVBM system Requirements, that the system shall not have the capability, including an optional capability, to use a remote server to mark a voter's selections, transmit it to the server from the voter's computer via the internet, store any voter identifiable selections on any remote server, or tabulate votes. And it was verified that, as I mentioned a little bit earlier, that once the ballot is delivered to the voter's personal environment, all connections are removed and there are no remote servers to do any of those things.

And that basically concludes --

MS. LAPSLEY: Okay.

MR. SANTOS: -- SLI's report.

MS. LAPSLEY: Great. Thank you, Mike.

So with that, is anyone -- is there anyone from Dominion that would like to respond to either the Staff Report or the consultant's report?

UNIDENTIFIED MALE: No, thank you.

MS. LAPSLEY: No, thank you? All right.

With that, we'll go ahead and move to public comments. And right now we have one public speaker card and that's from Mr. Fred Nisen with Disability Rights of California.

Mr. Nisen?

UNIDENTIFIED MALE: Thank you. We're from Disability Rights California, and I'm going to be reading his testimony.

(On behalf of Fred Nisen.)

"Hi. My name is Fred Nisen. I am the Supervising Attorney of the Voting Rights Practice Group at Disability Rights California, California's protection and advocacy system for people with disabilities.

"I, along with other members of my staff, participated in the testing of Dominion's ImageCast Remote 5.2. After reading through the reports online, these are my following comments.

"This PIN process is too cumbersome. It would require the voter have to have some dedication to not give up during this process. I understand that people are concerned with security at this time. However, just giving people more hoops to jump through will not make the system more secure and will scare away people who could benefit from having vote-by-mail be made accessible to them without having to waive their right to a private and independent vote. I have a reason to believe that Dominion is willing to work with counties to make their process less burdensome for voters with disabilities.

"As a condition of approval, the Secretary of State's

Office should require that the voter verification be a one-step process, asking for voter I'D, name and date of birth, similar to other RAVBM systems.

"Personally, I found the system easy to use, once I was able to get to the ballot. However, one of our staff members who uses the Java screen reading software on his computer also tested the system, including the problems with the audio instructions on how to complete a write-in candidate selection. He also found a problem with the audio instructions on how to return to the previous screen.

"I also noted in the Staff Report that the Secretary of State's Office expects counties to remake all the ballots that come in using this Remote Accessible Vote-By-Mail System. It is my understanding that when counties are using an ImageCast Voting System, as well as ImageCast Remote 5.2, they can simply be slipped into the ballot box when it is removed from the envelope. This would make the voter's choices as private as any other vote-by-mail voters since they do not have to use copy to a paper ballot.

"In fact, I understand that a county that uses Dominion ICX Ballot Marking Device as their accessibility voting system can use the ICX to duplicate the remote ballot. I am not advocating that

a county purchase a particular system, but if a county uses ImageCast to count their ballots and they use this Accessible Vote-By-Mail System, they should be able to input the Accessible Vote-By-Mail ballots directly into the ballot counter. This would ensure that the voter has a private and independent ballot to the ballot box without anybody filling out a ballot for them.

"Thank you."

MS. LAPSLEY: Great. Thank you.

Thank you, Mr. Nisen.

Seeing no other members of the public wishing to have -- to make public comment, we will be accepting public comment through May 6th, again, as I indicated before, to the Voting Systems at sos.ca.gov email address. People can feel free to send them electronically, or via U.S. Mail to Secretary of State, Attention: Voting System Comment, 1500 11th Street, 6th Floor, Sacramento, California 95814.

And that with, we'll go ahead and conclude this public hearing. Again, I thank everyone for coming and for your time today. Thank you.

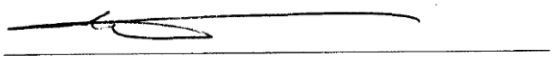
(The hearing concluded at 9:39 a.m.)

REPORTER'S CERTIFICATE

I do hereby certify that the testimony in the foregoing hearing was taken at the time and place therein stated; that the testimony of said witnesses were reported by me, a certified electronic court reporter and a disinterested person, and was under my supervision thereafter transcribed into typewriting.

And I further certify that I am not of counsel or attorney for either or any of the parties to said hearing nor in any way interested in the outcome of the cause named in said caption.

IN WITNESS WHEREOF, I have hereunto set my hand this 10th day of May, 2018.



PETER PETTY
CER**D-493
Notary Public

CERTIFICATE OF TRANSCRIBER

I do hereby certify that the testimony in the foregoing hearing was taken at the time and place therein stated; that the testimony of said witnesses were transcribed by me, a certified transcriber and a disinterested person, and was under my supervision thereafter transcribed into typewriting.

And I further certify that I am not of counsel or attorney for either or any of the parties to said hearing nor in any way interested in the outcome of the cause named in said caption.

I certify that the foregoing is a correct transcript, to the best of my ability, from the electronic sound recording of the proceedings in the above-entitled matter.

May 10, 2018

MARTHA L. NELSON, CERT**367