This has been submitted
votingsystems@sos.ca.gov

To Whom It May Concern:

RE: LA VSAP Certification

My name is Jim Soper. I am co-chair of the National Voting Rights Task Force and am writing on their behalf. I am also a senior software consultant with 35 years of experience, including with mobile devices.

First, we would like to thank Mr Logan for sending on quickly design specs for the printer system, and an explanation of how to deconstruct their QR codes. These proved to be very helpful and we posted them on our FB page (https://www.facebook.com/groups/VrtfCa/permalink/2737511793008373/?comment_id=2737514373008115) and sent them on to elists across the state.. We also would like to thank Mr Logan for his readiness to talk with us. We know that he is more than busy, so this is appreciated. We also note that he has involved the public into the design and testing of this system much more than we've seen from any private system. This has made for a less flawed system.

Much has been written about the technical aspects of the LA VSAP system, which we have posted here: https://www.facebook.com/groups/VrtfCa/permalink/2737511793008373/
We are not going to revisit all of them in detail, as they have been well covered by others.

In general, recognizing that the primaries are but weeks away, we cannot recommend immediate complete decertification as that would cause chaos, probably nationwide. LA County is too big and too complex to try to switch it over completely to another system in a few weeks. We do however, urge conditional approval, with the conditions designed to mitigate vulnerabilities and reduce public distrust of a flawed system. Some could be done quickly - the 4 contests per page problem.Others will take more time. They should be in place by November.

Some major issues:

Voting System Requirements
Staff report, issues 1 - 4, "Non-compliance with voting system requirements".
The response is sometimes "A discussion with the State is requested."

The NVRTF urges conditions be placed on these issues until such time as they can be put into place and reviewed by the public and/or independent specialists. There should be a deadline on some of the conditions, such as June 30, to ensure that they are covered.

Root access

Staff report, issue #11 - 14

"Programmatic setting of permissions to highly open configuration, and source files are not deleted after being copied to destinations on cluster machines." Otherwise stated, anybody who has access to the password to the tally system has complete control of everything on that computer." This is far more dangerous than most people understand.

The county response is: "only administrators on the Tally system should be authorized on the environment." and "A procedure has been added to restrict file system permissions on these files post-install.""

The NVRTF response is "yes!". But the public does not know what the authorization rules/procedures are. They should be made public insofar as publishing does not add to the risks involved. Review by outside specialists should be required.

USB booting

The tally system allows for booting from a USB device, allowing for complete control of the entire system, with no checks. This is dangerous. The ability to do this should be limited to very few people, and the public should know what those limitations are.

QR codes

The system reads votes not from the names printed on the paper ballot, but from a QR code. QR codes themselves are obviously not voter verifiable, which violates state laws and regulations. It is not sufficient to say that the voter may take the ballot to any other VSAP voting machine and have the votes in the QR code confirmed. You are asking a secret system to verify itself. Some independent checking may be possible if the county publishes soon a list of all the candidates and ballot measures, along with the numbers associated with them in the QR code. With that information, independent programmers can create mobile apps for the public to use to check the QR codes. In the long term, the scanners should be able to read votes from the names on the ballot, and not from the QR code.

Printer

"Because all ballots in this system are paper based, there is a fully auditable and permanent record of the election."

This is misleading. When the voter using the VSAP system decides to cast their ballot, it passes for a last time through the printer housing on the way to the ballot box, without the voter being able to review that final ballot. The county says that the printer head lifts during this final pass (https://vsap.lavote.net/wp-content/uploads/2019/09/VSAP_BMD-paper-path.pdf). It is possible, though a bit tricky, to program the printer to not lift up, and to alter the ballot after the voter has last seen it. There is no way for the public to verify what happens. This renders an audit unreliable, as we cannot 100% confirm that the ballots reflect voter intent.

The VRTF suggests two mitigations - (1) place the printer in a transparent case so that the public may see what occurs inside, or (2) redesign the system so that the path to the ballot box is separate from that of printer. For example, by placing the ballot box in front, or otherwise configuring the path to the ballot box separately from the printer path.

Airgapped system
"The system is airgapped—that is, not connected to the Internet or connected to any other system that is connected to the internet. Air gap systems "
Staff Report, 3. Software Testing (Source Code) Review Summary, Point 10, Page 11
Airgapping - transporting information by a physical device such as USB stick - does not mean that the system is secure. The Stuxnet virus used over 10 years ago demonstrated that a virus can be installed on an external device such as a USB stick from a programmer's computer, connected to the Internet, which can then carry the virus over to the "airgapped" targeted system. The situation that comes to mind is that of persons preparing ballot definition files on their own computers, and then transferring those files to the EMS. The computer used to prepare such files must never be connected to the Internet at any time.

Ballot images
We have heard that the LA VSAP system takes and keeps images of all the ballots it sees. This is very good. San Francisco has already published their 200,000 ballot images from the November election (
https://sfelections.sfgov.org/november-5-2019-election-results-detailed-reports
Select the FINAL REPORT option.) Even though it is possible for those images to be manipulated, we believe that more information is better, provided that those imaqes are NOT used in official audits. We strongly urge the county to publish those images as soon as possible before certifying the election.

Ballots on demand
Allowing for hand-marking of paper ballots makes for a more secure system. Printed ballots are easier to duplicate and stuff into the system. Plus we have confirmation that a human has checked a paper ballot when they are marking it by hand. SB 450 section 4007, reduced the number of Angelenos who will receive hand marked vote-by-mail (VbM) paper ballots as compared to other counties that adopt the SB 450 system. This is essentially pushing voters to use the electronic system, where they may better trust a hand-marked ballot.
(1) The NVRTF encourages the legislature to rewrite section 4007 so that LA conforms with the rest of the state
(2) We also encourage the county to install ballot-on-demand devices in as many vote centers as possible before the primaries. They should be available in all vote centers by November.

Open source
The LA VSAP project has been claiming that this system will be open source, or at least disclosed source, for nearly ten years. An example from August, 2018 is here: "State Certifies LA County's New Open-Source Vote Tally System"
https://mynewsla.com/life/2018/08/21/state-certifies-la-countys-new-open-source-vote-tally-system/
Open/disclosed source means that there is a web address (URL) where one can find the source code. To date, no such URL exists, so this is NOT an open/disclosed source system. The VRTF

insists that the county cease advertising this system as open source until such time as the public can have access to read and test the source code.

Four contests per page
Various pieces of election code prohibit screens from "scrolling'. This has led to a problem where the system can only display 4 candidate names per page, which gives the first 4 candidates an advantage. The gubernatorial recall election had 135 candidates. Any voting system must be able to handle this.
We suggest, absent a better idea, removing the "Next" button altogether, and require the voter to page through the entire ballot. I (Jim Soper) call this "paging" and not "scrolling"

Sincerely,

Jim Soper
Co-Chair; National Voting Rights Task Force