ALEX PADILLA | SECRETARY OF STATE | STATE OF CALIFORNIA
OFFICE OF VOTING SYSTEMS TECHNOLOGY ASSESSMENT
1500 11th Street | Sacramento, CA 95814 | **Tel** 916.695-1680 | **Fax** 916.653.4620 | www.sos.ca.gov

VSAP 2.0 Staff Report Addendum

Summary

During the original testing of the VSAP 2.0 voting system, multiple anomalies and vulnerabilities were identified during various phases of testing. Subsequently, the Secretary of State provided the County of Los Angeles the opportunity to mitigate and/or respond to the findings. The findings and subsequent mitigations required additional verification and/or documentation prior to certification. This information is outlined below.

Regression Updates and Mitigations

CVSS Sections 2.3.3.3 f and 3.2.2.1: Overvote Warning

An anomaly was identified during the functional and accessibility test phases, that CVSS Sections 2.3.3.3 f and 3.2.2.1 were not adhered to, by not warning voters of overvotes.

Resolutions: Subsequent verification of the ballot marking device system determined the functionality as designed does meet the requirement, as a voter is warned of overvotes by the indication of the counter in the middle right-hand corner of the screen indicating how many selections are left. Additionally, the voter is not allowed to make any further selections, until the voter deselects one of the previous selections. In a vote for one contest if the voter selects another choice, the previous choice is deselected, thus preventing an overvote. If a contest has the option to vote for more than one, for example vote for two or more, the voter can select up to the allowed number of selections. However, to change a selection, upon selecting the maximum allowed, the voter must deselect one of the previous selections.

USB/Root Vulnerability: Root access to the system through USB ports.

This USB vulnerability was related to the VSAP Ballot Layout (VBL) and VSAP Tally (Tally), not the VSAP Ballot Marking Device (BMD). All attempts to circumvent the physical security of the BMD itself through the USB port were unsuccessful. The BMD is not bootable.

Mitigations: The County has adopted procedures to limit root access to the VSAP system. The Tally Operations Center, where VBL and Tally are located, has multiple layers of physical security, including keycard access, video surveillance, and security personnel. The County generated a new set of cryptographic keys after FCMG completed this work and report, and incorporated them into a Trusted Build, locking out

Smartmatic and Digital Foundry staff. Only authorized County staff have system access, which would be necessary to exploit root access. These countermeasures significantly lessen the opportunity to exploit unauthorized root access. Furthermore, port locks have been placed on all USB ports in these locations to further reduce the risk.

Ballot Jams: Paper jams at the printer exit on the BMD

Mitigations: The issue was addressed through hardware and firmware changes to the BMD. The changes were submitted to and tested by SOS and FCMG. All changes passed review and regression testing. There were two changes:

1. Hardware:

Addition of metallic brushes that remove electrostatic energy that is created by the movement of the paper exiting the BMD into the ballot box; and

Addition of a mechanical guide to the paper ballot to ensure the ballot moves toward the rear side (the side away from the BMD) of the ballot box as it falls away from the BMD printer exit. This ensures that the ballots fall to the bottom and stack toward rear side of the ballot box.

2. Firmware:

The printer manufacturer provided firmware in the printer was updated to eject the ballot at a higher speed. This, along with the anti-static measures, helps ensure the ballot falls to the bottom of the ballot box. When the ballot remains in the printer exit (meaning it has not fallen into the ballot box) the printer sensors “see” it and give an indication that the printer is jammed.

Tamper-Evident Seals: Integrated Ballot Box (IBB) on the BMD may be opened and ballot removed/added without detection.

For this vulnerability to happen, a malicious actor must, without being noticed, access the back of a BMD for a prolonged period. They must have tape, tweezers and a piece of cardboard and they must maneuver carefully not to trigger a sensor on the ballot box that alerts Election Workers that the ballot box has been opened. This testing was conducted on a BMD without the attached privacy shield, which is an additional layer of protection to the attack.

Mitigations: The County has procedures in place to prevent this issue

1. Election Workers are trained to securely lock BMDs with serialized zip-tie seals;
2. Election Workers are trained to check seals and observe voting area for individuals who may be tampering with BMDs; and
3. Addition of adhesive tamper-evident seals placed over the seam of the IBB in addition to the serialized zip-tie seals that are used to securely close the box

As voted ballots will be removed every night by Election Workers, this attack would need to be conducted during the hours that a Vote Center is open and in operation, which would make the likelihood of an attempted attack or exploit highly unlikely without detection and disruption in the Vote Center. There are Vote Center personnel assigned as Voting Area Monitors who are responsible for observing and being present in the voting area where the BMDs are located. Not only would these workers notice someone working behind a BMD, but also, removal or opening of the ballot box triggers a screen display warning and requires Election Worker engagement to bring the triggered unit back into service. BMDs are also visible to all Election Workers and voters. The addition of the adhesive tamper-evident seals provides an additional layer of detection and protection.

"MORE" Button: Candidates who are not visible on first screen of contest may be at a disadvantage because voters may not see that they need to select the "MORE" button to see additional candidates.

Mitigations: The County consulted with its design and usability experts and with its development/manufacturing team to make refinements and modifications. These included:

1. Addition of a pulsating yellow ring to the "MORE" button; and
2. Addition of a gradient effect to visibly indicate that the contest continues vs hard page stops that appear that all options are visible in a single view

The County will also be promoting the use of the "MORE" Button through its voter education and outreach plans. The topic will be highlighted in the Official Sample Ballot, video tutorials, and informational displays and handouts at Vote Centers. Additionally, Election Workers will be trained on the issue in the event that voters need assistance.

Conclusion

Based upon the verification of functionality and review of documentation provided to the Secretary of State's office by the County of Los Angeles, the functionality and subsequent mitigations provided are satisfactory. The system is compliant with CVSS Sections 2.3.3.3 f and 3.2.2.1 respectively, additionally the County of Los Angeles has implemented and documented mitigations/resolutions to the findings as outlined above.