January 20, 2020

The Honorable Alex Padilla
Secretary of State
1500 11th Street
Sacramento, CA 95814

RE: Public comments regarding the proposed certification of Voting Solutions for All People 2.0 (VSAP)

Dear Secretary Padilla,

The National Election Defense Coalition (NEDC) is a national, non-partisan, not-for-profit organization founded in California, committed to promoting secure, transparent, accessible and trustworthy election systems and procedures. Free Speech For People is a national public interest organization dedicated to defending our Constitution and our democracy. We respectfully submit public comments with regard to the prospective certification of Los Angeles County's Voting Solutions for All People 2.0 (VSAP).

The State published the independent testing authority reports on VSAP on Friday, January 10, 2020, a short ten days before the close of the public comment period affording the public an exceptionally short period of time to review, study and comment on the test reports. Nevertheless, we have examined the test reports which document multiple issues of non-compliance with the California Voting System Standards include distinct failures of the Open Ended Vulnerability Testing (OVET fail), (which we enumerate below) that should decidedly disqualify the VSAP from receiving certification under California state rules. **While we recognize that VSAP was initiated and developed with highly admirable goals of accessibility for all voters, we respectfully urge the Secretary of State to withhold certification from VSAP until it can be brought into compliance with the California Voting System Standards (CVSS). Furthermore, VSAP should not receive certification until the areas of non-compliance have been remediated fully, and the modified system is re-tested by an independent testing authority to independently and transparently establish conformity with the CVSS.**

We note that the State staff report recommended certification of VSAP and we respectfully and vigorously disagree. We hold profound concerns that the State staff report has not adequately absorbed the gravity and severity of some of the issues of non-compliance with the CVSS regarding security that have been catalogued by the testing lab. The State staff report has dismissed many major security vulnerabilities that violate the CVSS as "low" or "no" severity.

We do not agree with many of these characterizations which appear to be founded, partially or fully, on assertions that the vulnerability could not reasonably be exploited because of physical security, air-gapping, presence of election workers or other procedures. This approach is faulty at best, dangerously naïve at worst. These requirements were drafted to provide robust protections for California's voting systems in all circumstances, including insider attacks, and it must be recognized that procedural protections cannot be guaranteed or relied upon. Furthermore, the CVSS were drafted with the expectation that voting systems would be air-gapped and be subject to physical security and election worker oversight. To disregard mandatory, robust standards in the CVSS by summarily declaring core security requirements as unnecessary is unsafe and especially reckless knowing that foreign adversaries are actively targeting our election systems for attack.

We are aware that the County and vendor have had a call with its Technical Advisory Committee to allay growing concerns that VSAP is non-compliant with the CVSS and violates several critical security requirements. We are also aware that the County and the vendor have assured the Committee that it has addressed the issues of non-compliance with the CVSS however, the County and the vendor did not provide any documentation or evidence to support these assertions. This is plainly inadequate. We are encouraged to know that the County and the vendor have recognized that there are critical failures that need to be corrected, however any changes to the system must be clearly documented and independently tested to ensure the corrections actually resolve the problems identified. No voting system should be certified until there is an itemized list of remediations which has been vetted by the same testers who identified the problems. That's just common sense.

The VSAP's failure to conform with core security requirements of the CVSS is especially troubling given that conformity with the CVSS was a central requirement of the extensive contract between Los Angeles County and the vendor, Smartmatic USA Corporation. According to the contract an objective of "Phase 2" of the VSAP development was specifically to result in confirmation that VSAP will result in CVSS Compliance. Further, the contract specified and expended for a certification/compliance specialist responsible for ensuring not just mere compliance with the CVSS, but that the CVSS would drive the design and development of VSAP, specifying:

> *The Certification/Compliance Specialists will be present at scrum meetings to ensure the CVSS requirements are being considered prior to code being created and will participate in code review to ensure proper coding conventions were adhered to. The Certification/Compliance Specialists will serve as a daily resource to the engineers (who are following a TDD process), so that unit and functional tests are designed from the beginning to comply with CVSS requirements. In such a way, CVSS compliance will be woven directly into the DNA of the code.*[1]

[1] Contract between Los Angeles County and Smartmatic USA Corporation. https://www.lavote.net/docs/rrcc/board-correspondence/06122018.pdf

VSAP's non-compliance with multiple critical security standards not only belies the claims that the CVSS would be "woven" directly into VSAP, it raises other questions regarding the vendor's compliance with the contract and commitment to the CVSS and system security.

Issues of non-compliance

We have enumerated several serious issues of non-compliance below. This is by no means a complete list but illustrates some serious issues that must be corrected and validated before VSAP should be certified.

CVSS 4.1.4.2.d.iii:

"Ballot boxes and ballot transfer boxes, which serve as secure containers for the storage and transportation of voted ballots, shall provide specific points where ballots are inserted, with all other points on the box constructed in a manner that prevents ballot insertion."

Testing lab finding: ***It is possible to insert or remove ballots from both the BMD and ballot transfer boxes without detection.***

CVSS 7.2.2.b: "Voting system equipment that implements role-based access control shall support the recommendations for Core RBAC in the ANSI INCITS 359-2004 American National Standard for Information Technology- Role Based Access Control document."

There is no evidence in the Technical Data Package to indicate that role-based access control, conforming to the recommendations of the Standard is implemented.

CVSS 7.2.4.a: "Voting systems shall ensure that only authorized roles, groups, or individuals have access to election data."

Too many functions require access to the root password. Also, a USB boot will give access to the election definition.

CVSS 7.3.b: "Voting systems shall only have physical ports and access points that are essential to voting operations and to voting system testing and auditing."

The unrestricted access to, and the ability to boot from, the USB port allows access to voting data.

CVSS 7.4.6. e.viii: "The minimum information to be included in the voting system equipment log shall be a cryptographic hash of the software update package using FIPS 1402 level 1 or higher validated cryptographic module".

The system does not use FIPS 140-2 validated cryptographic modules.

CVSS 7.4.6.f.i: “If the process uses hashes or digital signatures, then the verification software shall use a FIPS 140-2 level 1 or higher validated cryptographic module.”

The system does not use FIPS 140-2 validated cryptographic modules.

CVSS 7.5.4.a.iv: “OEVT fail criteria: violation of requirements - The voting device shall fail open ended vulnerability testing if the OEVT team finds vulnerabilities or errors in the voting device that violate requirements in the Standards. While the OEVT is directed at issues of device and system security, a violation of any requirement can lead to failure. The S-ATA shall report an OEVT failure if any of the following are found: Ability to modify electronic event logs without detection.”

The testers were able to gain access to the electronic event logs.

In addition, the testers found that booting from a USB drive was not disabled on any of the systems. As such, gaining physical access to the machines allowed access to both the operating and application files for VBL, Tally and FormatOS. This attack could be conducted by an election official insider or a vendor insider.

These issues are not minor infractions, they present significant security gaps that must be corrected. California is known to have some of the most robust voting system testing and certification requirements but these requirements are meaningless if the State does not enforce them. We urge the State to insist that any all violations of the CVSS that need remediation, be thoroughly and adequately addressed and independently tested to confirm compliance before the VSAP is certified.

Thank you very much for the opportunity to comment and for your consideration. We stand ready to answer any questions and help in any way.

Very Respectfully,

Susan Greenhalgh
Vice-President of Policy and Programs
National Election Defense Coalition

John Bonifaz
President
Free Speech For People