CENTER FOR DEMOCRACY & TECHNOLOGY

December 10, 2019

Alex Padilla
California Secretary of State
1500 11th Street
Sacramento, CA 95814
secretary.padilla@sos.ca.gov

Re: Proposed Regulatory Action on Risk-Limiting Audits

At the Center for Democracy & Technology (CDT), we work to preserve the user-controlled nature of the internet and champion freedom of expression. In the United States, voting is one of the ways in which citizens exercise their right to choose how their voice is represented in government. That is why protecting the election process is critical to the functioning of our democracy. The Election Security and Privacy Project[1] at CDT has three components in order to achieve the goal of improving election security. The first is providing basic to intermediate cybersecurity education for local election officials. The second is building bridges between election officials and the information security communities, and the third is advocating for post-election risk-limiting audits (RLA). Together with partners at the Center for Technology & Civic Life and the Democracy Fund, we have taught hundreds of election officials an "Election Cybersecurity 101" course and a course on post-election auditing and risk-limiting audits[2] because state and local election officials remain the front-line defense against election interference.

California should be commended for recognizing the potential for post-election audits to deliver higher levels of accountability at a lower cost. Election administrators across the country face a number of challenges in rolling out RLAs, and this proposed regulatory action is an example of how some of those challenges can be addressed at the state level by breaking down traditional manual tally requirements and providing an actionable framework to conduct fair and open RLAs. Along with states like Michigan[3] and Rhode Island[4], California can lead the way by publicly sharing the results of RLA pilots. Effective RLAs require a trustworthy audit trail – today, that means paper[5]. Tomorrow, that may include encrypted images or other records as a resulting of developments in mobile voting efforts, starting with UOCAVA voters or voters with accessibility needs. Such research would support the continued development and refinement of RLA methods and deployments.

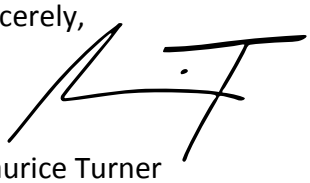
In my opinion, deterrence is one of the most underreported benefits of RLAs. An attacker benefits when only a small number of contests are selected for auditing. The attacker knows that they can

[1] https://cdt.org/issue/internet-architecture/election-cybersecurity/
[2] https://www.techandciviclife.org/online-series
[3] https://www.brennancenter.org/our-work/research-reports/review-robust-post-election-audits
[4] https://www.verifiedvoting.org/wp-content/uploads/2019/09/RI-Report.pdf
[5] https://www.nytimes.com/2019/11/30/us/politics/pennsylvania-voting-machines.html

CENTER FOR DEMOCRACY & TECHNOLOGY

avoid those specific contests if the contests are identified before voting or take the chance that they can target a contest not likely to be selected at random. By continuing to refine techniques, build local election official expertise, and reduce costs, RLAs can be conducted on every contest in every jurisdiction and would make interference a costly and risky proposition for foreign and domestic attackers.

Sincerely,



Maurice Turner
Deputy Director, Internet Architecture Project