



SHIRLEY N. WEBER, PH.D.
CALIFORNIA SECRETARY OF STATE

September 10, 2021

Mustaque Ahamad
Professor, School of Cybersecurity and Privacy, Georgia Tech

Duncan Buell
NCR Chair in Computer Science and Engineering (Emeritus), University of South Carolina

Richard A. DeMillo
Charlotte B. and Roger C. Warren Professor of Computer Science and Chair, School of Cybersecurity and Privacy, Georgia Tech

Candice Hoke
Founding Co-Director, Center for Cybersecurity & Privacy Protection, Cleveland-Marshall College of Law, Cleveland State University

Harri Hursti
Co-founder, Nordic Innovation Labs; Co-founder, Voting Village at DEFCON

David Jefferson
Retired Computer Scientist, Lawrence Livermore National Laboratory

Wenke Lee
John P. Imlay Professor of Computer Science; Director Georgia Tech Cybersecurity Center; School of Cybersecurity and Privacy; Member, Georgia Commission on Safe Secure Elections

Prof. Philip B. Stark
Professor, Department of Statistics, University of California, Berkeley

Dear Professor Ahamad, Mr. Buell, Professor DeMillo, Ms. Hoke, Mr. Hursti, Mr. Jefferson, Professor Lee, and Professor Stark:

Thank you for your September 2, 2021, correspondence.

Recently the Colorado Secretary of State announced a security breach of Mesa County's voting equipment, where the Mesa County Clerk allegedly provided an individual

1500 11TH STREET, SACRAMENTO, CA 95814, (916) 653-7244

WWW.SOS.CA.GOV



September 10, 2021

Page 2

unauthorized access to the county's voting system. Following the unauthorized access, images of the voting system's hard drive and Basic Input/Output System (BIOS) passwords were posted on Gateway Pundit, a conspiracy news site. The breach is currently under investigation by the Colorado Secretary of State, the FBI and the Mesa County District Attorney's office.

Thank you for meeting with me and my staff yesterday, September 9, to discuss your letter to me. As articulated during the meeting, the Colorado breach is very serious. California has security measures in place, which includes manual tally audit, based on the assumption that there are bad actors who may attempt to gain unauthorized access and breach our systems.

My office has worked by your side for years to formulate and implement the strictest safety and security protocols to keep California's voting technology safe and free from interference. Our most recent collaboration has centered around Risk Limiting Audits (RLAs) in California. Your collective expertise and that of other RLA experts has led to the Legislature's sign off and our implementation of an RLA Pilot Program which has only just begun.

When we worked together to create the RLA Pilot Program, you understood the goal: to effectively bring on all 58 counties by the end of the program in 2023 to ensure a smooth transition.

As you are aware, risk limiting auditing is allowed in California under Elections Code section 15367 which provides: "commencing with the statewide primary election held on March 3, 2020, the elections official conducting an election may conduct a risk-limiting audit in place of the one percent manual tally required by Section 15360 during the official canvass of any election in accordance with the requirements of this article." The statute is permissive, not mandatory. Our authority is defined by that statute.

Our office has and continues to support and advocate for risk limiting audits. We worked closely with the author (Assemblymember Quirk) and RLA proponents (including Professor Stark and other RLA expert) to develop, pass and implement the legislation. We spearheaded a working group (including Professor Stark and other RLA experts) to develop RLA regulations and a RLA tool for counties to use. RLA is a new auditing process which involves many steps and the use of the algorithm tool that we developed. Only a handful of counties have conducted RLAs for a small selection of contests in the primary election in March and the general election in November 2020.

Your request to mandate all California counties to implement RLA, almost all of them would be doing so for the first time, less than two weeks ahead of a statewide Gubernatorial Recall Election is not possible. As you are aware, implementation of RLA in each county requires significant preparation, training and testing. It is a different process

and procedure than the 1% manual tally that California counties have done for many years in every election. Further, the implication that California's elections cannot be conducted safely and securely without RLA is inaccurate, as California has the strictest voting system testing, procedures for use and security requirements in the nation.

While we understand the added value RLA brings to election validation, California's elections are already built upon a strong, secure foundation. California tests every step of its election processes with the assumption that a Mesa County-type incident could happen.

Security is built and layered into every aspect of California's voting technology, including but not limited to:

- California conducts source code review and evaluation, hardware and software security penetration testing, operational testing to validate system performance and functioning under normal and abnormal conditions and more to identify any vulnerabilities and have our voting systems resolve or mitigate them.
- Every California voter receives a paper ballot – which creates a voter-verified paper audit trail that provides voters an opportunity to review their choices when casting their paper ballot and provides elections officials with a means to confirm the accuracy of tabulation.
- California voting systems and tabulators -- including Dominion systems - ARE NOT connected to the internet, nor do they have modems or hardware in them that could be remotely "activated."
- California voting systems have physical intrusion prevention security controls and safeguards.
- California voting systems are installed only with trusted build software provided by the Secretary of State.
- Every county must validate - before every election - that the voting system is identical to the Secretary of State supplied trusted build by reinstalling the trusted build or utilizing the Secretary of State trusted build cryptographic HASH (essentially a digital fingerprint of the software and firmware) to ensure it matches the approved version and has not been modified.
- Ballot printers are regularly inspected and certified by our office.
- Vendors and county officials follow strict physical security and chain of custody requirements for all voting technology software, firmware and hardware which meet or exceed federal guidance including that of the Justice Department, the Cybersecurity and Infrastructure Security Agency and the Election Assistance Commission.
- If chain of custody has been compromised or attempted to be breached, the Secretary of State must be notified immediately, and investigation, verification, and sanitization (e.g. NIST Media Sanitization

guidelines <https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final>)
procedures be followed.

- County election officials must follow specific role-based permissions, administrative and management controls, access controls, security procedures, operating procedures, physical facilities and arrangements controls, and organizational responsibilities and personnel screening.
- Minimum password complexity, length, strength, and lock out policies for failed attempts is required. Under no circumstances may default passwords be used.
- Every county performs logic and accuracy testing.
- For every election, each county must conduct an audit by manual tally or risk limiting auditing to identify and resolve any discrepancies.

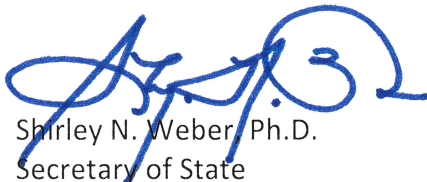
Additionally, we are in regular contact with and work closely with federal and state law enforcement and intelligence agencies to ensure we protect our elections. Should anyone attempt to interfere with our election we will work with state and federal law enforcement agencies to prosecute them to the full extent of law and hold them accountable.

Having heard from each of you as well as many other RLA and security experts, we will make more information and data about the 1% manual tally audits publicly available for this and future elections. My staff will be providing more information in the days to come.

We hope to continue to work collaboratively with all of you and other RLA and election security experts to continue to develop the RLA Pilot Program and ensure that it is implemented in California's counties successfully in the future. As always, I welcome your thoughts and open discussion on how California elections can be made even more secure and accessible in the future.

Californians should be confident that at the end of the day, their vote will count. Our office and county election officials take election security very seriously and will continue to do so for this election.

Sincerely,



Shirley N. Weber Ph.D.
Secretary of State