MARK MILLIMAN

August 5, 2021

Jena Griswold
Colorado Secretary of State
1700 Broadway, Suite 550
Denver, CO 80290

SUBJECT: TESTIMONY ON NOTICE OF PROPOSED RULEMAKING 8 CCR 1505-1

Dear Secretary Griswold:

Yesterday I delivered an oral testimony during the open part of the hearing, and this is the formal written submission to augment the statements I made during the hearing. I formally object to illegality of adopting these changes under the guise of emergency rules. I am not a lawyer and even I could see that what your office is trying to do is illegal under the laws of the State of Colorado.

My testimony focuses on two general items: third-party audits and vote management system security. None of my statements contradict any item mentioned in Senate Bills 21-188 and 21-250.

Rule 21.4 Voting System Standards

This rule is based on the obsolete 2002 Voting Systems Standards that is 20 years old. Technology and criminals have advanced tremendously during that period. Relying on these standards to maintain security of our voting systems is like letting the fox guard the hen house. Computer equipment, operating systems, peripherals, networking, and software development have developed exponentially as well as standard security practices.

Our elections should be held to military encryption and security standards because they are the most important things citizens do in this country and deserve the same protection as our national security. This rule should be modified to comply with the latest military security standards and updated as they are updated. Anything less is irresponsible.

Rule 21.5.1 Voting System Provider Demonstration

I do not have any issues with this rule other than it is of little value to prove the integrity and security of the Election Management System. It is essentially a *dog-and-pony show*. Illicit features, back doors, remote access, surveillance software, and other nefarious capabilities can be in the system without them being exposed during the demonstration. The demonstration should not be a substitute for a full complete functionality and security audit and certification by a professional security and penetration testing company.

4080 Greens Place • Longmont, Colorado 80503 • (720) 249-2737 • [redacted]@ieee.org

RULE 21.7.4

This rule attempts to disallow any third party from auditing or testing the integrity of the election management systems and vote counts. Competent and certified auditors and security certification companies should be allowed to have full access to ballots and EMS to conduct a forensic audit of any election. The chain of custody procedure should be modified to allow competent companies to complete a forensic audit.

Free, fair, and transparent elections will allow for a forensic audit of a race or races when necessary to preserve confidence in our democratic republic. Sometimes RLA are not sufficient when systematic fraud is suspected. Implementing this rule will offer validation that our elections may not be free and fair. There are several companies in the United States qualified to provide a safe and secure forensic audit without compromising the integrity of the machines. Part of the audit process would be to recertify the machines after the audit is complete.

Forensic audits should have access to the software images and source code in the machines to test verify the integrity and security of these systems. Offering this type of access provides a non-destructive way for a third party to conduct full security and penetration testing.

This and the next rule should be deleted at this time.

RULE 21.10

Rule 21.10.1 should include all source code as well as the individual images deployed on the machines. Each time new software of any type is provided to be installed on machines that software should be escrowed as well.

Modification to this rule allows third party security, testing, and certification companies to test software and review source code without actually impacting production machines.

CONCLUSION

The rules should be modified to conform to today's military standards for computer and network security. Relying on outdated standards does not guarantee the integrity of our elections. The Secretary of State's office should use recognized industry professionals and laboratories to test and certify our election management systems. The state does not have the expertise to make sure our systems are secure; therefore, it should rely on industry security experts to verify the integrity of the EMS, network it is connected, and the process surrounding the deployment and use of that system.

Our chain-of-custody procedures can be modified to allow competent third-party professional companies to conduct a forensic audit when necessary. Non-destructive testing and auditing of the software can be completed with escrowed software source code and images. Individual hardware can be inspected without destruction as well. If seals and cases are opened, the procedure can be modified to make that secure itself without destroying the machines. After the audit is complete, the machines will be wiped clean and recertified.

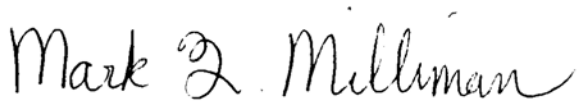
My recommendation is to delete the proposed changes to rules 21.4, 21.7.4, and 21.7.5 at this time. Modify rule 21.10.1 to include source code and any released software.

AUTHORITY

I am a degreed electrical engineer with a Master of Science from Carnegie Mellon University (home of the Software Engineering Institute). I have over 30 years' experience developing and selling telecommunications systems to telecommunication service providers around the world. In my last role at CapGemini Engineering, I was part of our security practice that developed products for carriers to use with our services to provide end-to-end security testing of every element in a carriers' network. Part of that practice provides security and penetration audits of networks to find vulnerabilities. The few recommendations I have made are based on that experience.

I welcome the opportunity to work with the Secretary of State's staff on ways to improve the security of our elections with the Election Management Systems. No matter how well-intentioned EMS vendors may be, they are not ultimately responsible for the integrity and security of our elections and sometimes their goals may not align with one person, one vote. I have read most of the statute on our elections and I have been learning more about our Election Management systems and how they are deployed in different counties. I have worked as a poll watcher and precinct captain in two Boulder County presidential elections under different County Clerks. In the 2020 election, I was a candidate for House District 11. We can definitely improve our processes to give voters more confidence that their votes actually count.

Sincerely,



Mark Milliman