Testimony: Rules Committee, Oregon State Legislature, April 10, 2019
Sheila Golden

Good afternoon. I'm a voting rights/election integrity activist and I'm here to speak on behalf of SB 944. This bill, if passed, would amend two current laws, ORS 254.529 and ORS 254.535, to allow post-election audits to be either fixed-percentage or risk-limiting audits. In addition, it requires that audits take place after every election, not just after general elections. Why do I think that these two changes are a good idea?

Let's start with the importance of post-election audits. Is Oregon's voting system vulnerable to attack? The answer is yes. The problem isn't only with the reliability of voting equipment, i.e. optical/digital scanners. There are vulnerabilities throughout the many parts of our complex voting system: in voter registration databases that are cyber-attacked almost daily; in election night reporting systems using the internet to transmit county vote totals to the state; in chain of custody practices requiring physical security for machines, votes and the counting of votes during elections; in the security practices of vendors supplying counties with voting software, hardware, technical support and more. And this is just a partial list!

In the fall of 2017, while working on an ACLU voting rights campaign, amid reports of threats to US voting systems, I decided to research Oregon's. The results were both reassuring and disquieting. On the one hand, I found many built-in safeguards that keep elections secure. One example: though the internet is used on election night to send in county vote totals, the election night total is not the official record. Results are official only after the post-election audit, which can correct the earlier total if need be, and then mailed to the state as hard copies.

On the other hand, I found that optical/digital scanners are definitely hackable: the software running them is produced and updated by other computers that are or could be Internet-connected and unsecured. If these computers have been infected with malware, it can easily spread to the voting software they're producing. And, once ready, the corrupted software can be installed in voting equipment without any Internet connection needed, by using removable media (i.e. flash drives and memory cards) for program installation and upgrades. Other ways of hacking include: through direct access, when someone physically present tampers with the scanner; through remote access, when someone isn't

physically present, but attacks through remote-access software installed in the scanner; through "phishing attacks" directed at election officials while they're online; through malware-infected chips and other parts coming from an unsecured supply chain. While some of Oregon's counties have IT staff to prevent/address such problems, many others have no IT staff, and rely on a small state security team.

Equally disturbing was discovering that two scanners currently used in Oregon, the DS 850 and the M650, both sold by ES&S, have additional serious vulnerabilities. The DS 850, a digital scanner used in Oregon since 2015, was vulnerability-tested by a California cybersecurity firm (Freeman, Craft, McGregor group) in 2016. They found 50 different vulnerabilities in the core part of the operating system, allowing the widest possible access to the whole system. On a scale of 0-10, all scored between 7-10. The M650, an optical scanner in use in Oregon since 2005, was vulnerability-tested in 2007 by The Everest Project, a study conducted for Ohio by a team of independent cybersecurity researchers. They found that an outside attacker, using a forged update disk, could take total control of the M650 and use it to undetectably alter vote tallies, accept forged ballots, prevent attempted reprogramming and many other disruptions. While I was told that counties report bugs to vendors, I wasn't able to find out if these particular problems had been resolved. Finally, the age of the M650s, between 10-14 years, is problematic. Most voting machines are meant to last about 10 years; after that, malfunctions become more and more likely.

Overall, this is a mixed picture: a voting system that does a great deal to ensure that voting is fair and secure, but one that has some parts with the potential to completely undermine those goals. What to do? The answer is already in place: conduct meaningful post-election audits. Even with the best efforts, any system can falter or fail, and the only way to know when it does is to hand check its results against a paper record, and to do so for every election.

As of now, that audit uses a fixed-percentage method which counts more votes when the margin of victory is narrow, and fewer if the margin widens. It's an effective method that was considered best practice in 2007, the year ORS 254.529 became law. Since then, however, a newer method, the risk-limiting audit, has been developed. What I like about risk-limiting audits is the strong certainty they offer that if the vote tabulation system found the wrong winner, the audit will reveal the correct winner. So if, for example, an auditor chooses a 90% risk limit and the machine-reported vote count is incorrect, there is a 90%

chance that the audit will detect the incorrect outcome and reveal the correct one. RLAs are currently seen as the gold standard of audits and as such, they should be available as an audit option. SB 944 would enable individual counties to pilot RLAs, while letting others continue to use fixed-percentage audits if they choose to. A good way for those who are curious but not ready to become familiar with RLAs.

In sum, the current law already recognizes that post-election audits are the necessary partner to a system based on machine-counted paper ballots. SB 944 strengthens that partnership by adding a new, effective way to audit, and by requiring audits for all elections.

Thank you.