

**Statement of Liz Howard
Cybersecurity and Elections Counsel
Brennan Center for Justice at NYU School of Law**

**Ohio Senate Government Oversight and Reform Committee
May 6, 2018**

The Brennan Center thanks Chairman Coley, Vice Chair Uecker, Ranking Member Schiavoni and members of the Senate Government Oversight and Reform Committee for the opportunity to provide written testimony in support of Senate Bill 256 today. The Brennan Center is a nonpartisan law and policy institute that works to reform, revitalize – and when necessary, defend – our country's systems of democracy and justice. For over a decade, we have studied America's election infrastructure and promoted common-sense policies to protect and secure our electoral system.

Senate Bill 256 would mandate Risk Limiting Audits throughout the state by 2020. In doing so Ohio would adopt a critical security measure recommended by many of the nation's leading election integrity experts, and join a growing number of jurisdictions in requiring a post-election process that employs statistical models to provide a high level of confidence in the accuracy of the final vote tally.

The reason that so many jurisdictions are turning to Risk Limiting Audits is simple: such audits are a critical way to ensure that a hack, software bug or programming error cannot change the outcome of an election, and are a transparent means for providing the public with evidence of the integrity of our elections.

Adding a Statutory Requirement for Risk Limiting Audits Is an Important Security Step

Ohio already has a number of critical protections in place to prevent or detect cyberattacks against its voting machines, such as mandatory pre-election logistics and accuracy testing on all voting equipment,¹ auditable paper trails of every vote cast, and post-election audits required by the Secretary of State.²

However, the race against cyberattacks is one without a finish line. Even systems not connected to the internet are vulnerable to viruses and malware spread through portable memory devices.³ Furthermore, sophisticated software attacks can be designed to be inactive and undetectable during pre-election testing. Given the warnings of national security experts that Russia and other nation states may target American elections in the future, we cannot discount the possibility of such attacks.⁴ While most audits currently conducted in Ohio might catch sophisticated attacks, they are not designed to do so.

By contrast, Risk Limiting Audits are designed to detect all types of intentional attacks, unintentional errors and any other causes that result in an incorrect election outcome. These customized audit processes employ proven statistical models to consistently and efficiently provide a high level of confidence in the accuracy of the election outcome.

¹ Ohio Rev. Stat. § 3506.14, available at <http://codes.ohio.gov/orc/3506.14v1>.

² Ohio Election Official Manual § 9-29 (May 2016), available at https://www.verifiedvoting.org/wp-content/uploads/2017/09/OH_2015eom.pdf.

³ *The State and Local Election Cybersecurity Playbook*, Belfer Center for Science and International Affairs (February 2018), <https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook#app1>.

⁴ See Daniel R. Coats, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," testimony before the Senate Select Committee on Intelligence (February 13, 2018), available at <https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-021318.PDF>.

Experts Recommend Adoption of Risk Limiting Audits

Numerous national experts have recommended the adoption of Risk Limiting Audits.⁵ The U.S. Senate Select Committee on Intelligence, which held multiple hearings related to Russian interference in the 2016 elections, formally recommended that states, “consider implementing more widespread statistically sound audits of election results,” and noted, “[r]isk limiting audits, in particular, can be a cost-effective way to ensure that votes cast are votes counted.”⁶ Congress provided additional support for RLAs when it allocated \$380 million for states “to make election security improvements” and expressly identified “[i]mplement[ing] a post-election audit system that provides a high level of confidence in the accuracy of the final vote tally” as a permissible grant expense.⁷ Senate Bill 256 would make Ohio elections more secure by implementing this agreed-upon “gold standard” of post-election audits.

For the same reasons, Risk Limiting Audits have been embraced and recommended by many others, including former U.S. Department of Homeland Security Secretary Michael Chertoff; former Kentucky Secretary of State Trey Grayson; former West Virginia Secretary of State Natalie Tennant; Joseph Hall, Chief Technologist, Center for Democracy and Technology; and Ronald Rivest, MIT Vannevar Bush Professor of Electrical Engineering and Computer Science.⁸

An Increasing Number of Jurisdictions Around the Country Are Adopting Risk Limiting Audits

In light of these facts, it should be of no surprise that several jurisdictions around the country have recognized the necessity of adopting Risk Limiting Audits as a critical security measure.

⁵ See *Federal Funds and Difficult Decisions*, The Canvass, National Conference of State Legislatures (May 2018), <http://www.ncsl.org/research/elections-and-campaigns/the-canvass-may-2018.aspx> (summarizing recommendations by the U.S. Election Assistance Commission, Center for American Progress, Multiple Experts and Defending Digital Democracy); Lawrence Norden and Christopher Famighetti, *America’s Voting Machines at Risk* 32 (2015), Brennan Center for Justice, available at <https://www.brennancenter.org/publication/americas-voting-machines-risk>; Mark Lindeman & Philip B. Stark, *A Gentle Introduction to Risk-Limiting Audits* (2012), available at <https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf>; *Principles and Best Practices for Post-Election Audits*, ElectionAudits.org (September 2008), http://electionaudits.org/files/bestpracticesfinal_0.pdf; *Post Election Audits, Verified Voting*, available at <https://www.eac.gov/assets/1/28/VerifiedVoting-Post-Election-Audits.pdf>; Statement on Risk Limiting Post-Election Audits, Am. Statistical Ass’n (2010), available at https://www.amstat.org/asa/files/pdfs/POL-Risk-Limiting_Endorsement.pdf.

⁶ Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations, U.S. Select Senate Committee on Intelligence (May 8, 2018), available at <https://www.intelligence.senate.gov/publications/russia-inquiry>.

⁷ See Consolidated Appropriations Act of 2018, Pub. L. No. 115-141, 132 Stat. 348 (authorizes and appropriates the federal funds); see also “Division E – Financial Services and General Government Appropriations Act, 2018,” available at https://www.eac.gov/assets/1/6/2018_HAVA_Funds_background.pdf (joint explanatory statement indicating congressional intent on how funds may be spent).

⁸ See “National Security, Tech, and Election Officials to States: Best Practices Should Guide How New Voting System Security Funds Are Spent,” Brennan Center for Justice (April 23, 2018), <https://www.brennancenter.org/press-release/national-security-tech-and-election-officials-states-best-practices-should-guide-how>; Michael Chertoff & Grover Norquist, “We need to hack-proof our elections. An old technology can help,” *Washington Post* (February 14, 2018), https://www.washingtonpost.com/opinions/we-need-to-hack-proof-our-elections-an-old-technology-can-help/2018/02/14/27a805bc-0c4b-11e8-95a5-c396801049ef_story.html?utm_term=.1c1a9edd8eee; Robert F. Bauer et al., *The American Voting Experience: Report and Recommendations of the Presidential Commission on Election Administration* (January 2014), available at https://www.americanbar.org/content/dam/aba/administrative/state_local_government/Voting.authcheckdam.pdf.

In 2017, Colorado completed the first-of-its-kind statewide Risk Limiting Audit.⁹ Last year, the Rhode Island legislature followed Colorado's lead and passed its own statewide requirement for RLAs.¹⁰ Meanwhile, Marion County, Indiana just completed a successful RLA pilot last month and multiple localities in Virginia, California and across the country are planning to conduct pilots this summer and after the November 2018 election.

The Committee Should Consult with Additional Experts

We were pleased to learn that the Committee will receive testimony from Patrick McDonald, Director of the Cuyahoga County Board of Elections, who has overseen Risk Limiting Audits. While lessons from Cuyahoga County will no doubt be helpful, we urge the Committee consult with experts and election officials across the country who have studied this issue in depth over the last few years and have experience and expertise with developing and conducting RLAs.

The Secretary Should Retain Broad Authority

Senate Bill 256 appears to strike a good balance by establishing important broad statutory principles to govern this process and by providing the Secretary of State with sufficient authority to develop practical policies and procedures. When drafting these procedures, the Secretary would also benefit greatly from consulting with security experts, legislators, and other election officials who have significant experience with creating and implementing RLA protocols. These policies and procedures should ensure that the audit is conducted in a manner that will increase public confidence in election results.

Conclusion

The Brennan Center supports common-sense policies that make our elections more secure. Senate Bill 256 would mandate one of those policies: Risk Limiting Audits. In the months ahead, we look forward to future opportunities to share with the committee in greater detail our thoughts about how this and other policy reforms can increase transparency, security and confidence in Ohio elections

⁹ See Dwight Shellman & Jennifer Morrell, "Colorado's Implementation of Risk-Limiting Audits," U.S. Election Assistance Commission (October 13, 2017), <https://www.eac.gov/colorados-implementation-of-risk-limiting-audits/>.

¹⁰ RI Gen L § 17-19-37.4, available at <https://law.justia.com/codes/rhode-island/2017/title-17/chapter-17-19/section-17-19-37.4/>.

