BRENNAN
CENTER
FOR JUSTICE

**Committee on House Administration**
**United States House of Representatives**

**Statement of Lawrence D. Norden**
**Deputy Director, Democracy**
**Program,**
**Brennan Center for Justice at NYU School of Law**

**May 8, 2019**

**"Election Security"**

Chairperson Lofgren, Ranking Member Davis, and members of the Committee, thank you for the opportunity to speak about the critical issue of election security. The Brennan Center for Justice—a nonpartisan law and policy institute that focuses on democracy and justice—appreciates the opportunity to share with you the results of our extensive studies and efforts to ensure our nation's election systems are more secure and reliable. We are deeply involved in the effort to ensure accurate and fair voting for all Americans.

For more than a decade, I have led the Brennan Center's extensive work on voting technology and security. In 2005, in response to growing public concern over the security of new electronic voting systems, I chaired a task force (the "Security Task Force") of the nation's leading technologists, election experts, and security professionals assembled by the Brennan Center to analyze the security and reliability of the nation's electronic voting machines.[1] In the decade and a half since, I have authored or co-authored numerous studies on election system security and technology, including the results of a semi-regular Brennan Center survey of the nation's roughly 8,000 local election officials.[2]

Our most recent survey (published in March) showed that while officials have made great progress

[1] "About the Task Force on Voting System Security," Brennan Center for Justice, January 1, 2005, https://www.brennancenter.org/analysis/about-task-force-voting-system-security.

[2] *See e.g*. Lawrence Norden, *Post-Election Audits: Restoring Trust in Elections,* Brennan Center for Justice, 2007, https://www.brennancenter.org/sites/default/files/legacy/d/download_file_50228.pdf*;* Lawrence Norden, *Voting System Failures: A Database Solution*, Brennan Center for Justice, 2010, https://www.brennancenter.org/sites/default/files/legacy/Democracy/Voting_Machine_Failures_Online.pdf; Lawrence Norden and Christopher Famighetti, *America's Voting Machines at Risk*, Brennan Center for Justice, 2015, https://www.brennancenter.org/publication/americas-voting-machines-risk; Lawrence Norden and Ian Vandewalker, *Securing Elections from Foreign Interference*, Brennan Center for Justice, 2017, https://www.brennancenter.org/publication/securing-elections-foreign-interference; Lawrence Norden and Wilfred U. Codrington III, "America's Voting Machines at Risk – An Update," *Brennan Center for Justice*, March 8, 2018, https://www.brennancenter.org/analysis/americas-voting-machines-risk-an-update; Lawrence Norden and Andrea Córdova, "Voting Machines at Risk: Where We Stand Today," *Brennan Center for Justice*, March 5, 2019, https://www.brennancenter.org/analysis/voting-machines-risk-where-we-stand-today.

in the last two years toward improving election security, much work remains to be done.[3] In particular, local election officials around the country, underfunded and often without any local IT support, are on the front lines in the effort to protect our democracy against hostile actors, including foreign powers. They deserve leadership and resources from all levels of government.

I hope to convey three points in my testimony today:

(1) The United States has made important progress since 2016 in protecting its election infrastructure;
(2) While Special Counsel Robert Mueller's report confirmed a "sweeping and systemic" attack on American elections in 2016, there are several reasons to believe the threat against our election infrastructure will be even greater in 2020; and
(3) There is more to do to protect our elections in 2020 and beyond, and Congress has a critical leadership and partnership role to play.

## A. The Attack Against America's Election Infrastructure in 2016 and the Progress We Have Made Since

The redacted Report on the Investigation into Russian Interference in the 2016 Presidential Election by Special Counsel Robert S. Mueller III (the Special Counsel's Report) is a powerful reminder and warning, just 18 months before our next presidential election, that a foreign power engaged in a major effort to interfere in our elections. The Special Counsel's Report confirms the reports of our intelligence agencies, as well as the results of Congressional investigations, which have shown that in addition to a massive effort on social media, the Russians targeted state and local election boards, breached and extracted data from a state registration database, and used spear phishing attacks to gain access to and infect computers of a voting technology company and at least one Florida county.[4]

Yet there is good reason to believe we face even more serious threats in 2020 and beyond. In contrast to other Russian efforts during the 2016 election cycle, the attacks against our election infrastructure appear to have begun relatively late compared to other aspects of their campaign, with the first documented intrusions noted in June of 2016. By 2020, the Russians will have had four years to leverage knowledge gained in 2016 to do more harm. Chris Krebs, head of the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security, has warned that the 2020 election is "the big game" for adversaries looking to attack American democracy. [5]

We have seen the kind of damage Russian operatives can do with well-planned attacks against election infrastructure, such as the alleged attacks against Ukraine's elections in 2014, which deleted enough files to make the country's voting system inoperable days before the election,

[3] Lawrence Norden and Andrea Córdova, "Voting Machines at Risk: Where We Stand Today," *Brennan Center for Justice*, March 5, 2019, https://www.brennancenter.org/analysis/voting-machines-risk-where-we-stand-today.
[4] Robert S. Mueller III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, U.S. Department of Justice, 2019, 51, https://www.justice.gov/storage/report.pdf.
[5] Colleen Long and Michael Balsamo, "Cybersecurity officials start focusing on the 2020 elections," *Associated Press*, November 8, 2018, https://www.apnews.com/cfaa16f6a86349bebc16e0633d6214dd.

and which inserted a virus into the country's election night reporting designed to falsely declare an ultra-nationalist party as the victor.[6] We have seen similar attacks by alleged Russian operatives against Bulgaria's Central Election Commission during a referendum and local elections in 2015, as well as against Ukraine's election commission in 2019.[7]

Just as importantly, there are other nation-states that could attack our election infrastructure in 2020. U.S. national security agencies have warned of the potential for attacks against our elections from China, North Korea, and Iran, as well as non-state actors.[8] Since 2016, there have been reports of alleged Chinese election-related attacks against Indonesia's voter database[9] as well as against Australia's major political parties.[10]

There was a time when many assumed no nation-state would dare attack America's election infrastructure for fear of the consequences. We can no longer live under this illusion.

The good news is we have made significant progress since 2016 to secure our elections. Most importantly, policymakers and election officials around the country are acutely aware of the threat that hostile actors pose to the integrity of our elections. As a result, election officials and their employees have voluntarily participated in thousands of hours of cybersecurity trainings and table-top exercises to prevent, detect, and recover from intrusions into critical election infrastructure.[11]

The designation by the Department of Homeland Security ("DHS") of election infrastructure as critical infrastructure has meant that state and local election offices have had access to needed resources, including cybersecurity advisors and risk assessments. Meanwhile, DHS and the Election Assistance Commission ("EAC") have facilitated much better information sharing between election system vendors, the states, and the federal government.

Finally, in 2018 Congress provided $380 million in Help America Vote Act (HAVA) funds to help states bolster their election security. Based on information provided by the EAC, we know

[6] Andy Greenberg, "How an entire nation became Russia's test lab for cyberwar," *Wired*, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.

[7] Gordon Corera, "Bulgaria warns of Russian attempts to divide Europe," *BBC News*, November 4, 2016, https://www.bbc.com/news/world-europe-37867591; Pavel Polityuk, "Exclusive: Ukraine says it sees surge in cyber attacks targeting election," *Reuters*, January 25, 2019, https://www.reuters.com/article/us-ukraine-cyber-exclusive/exclusive-ukraine-says-it-sees-surge-in-cyber-attacks-targeting-election-idUSKCN1PJ1KX.

[8] *See, e.g.*, Daniel R. Coats, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*, Office of the Director of National Intelligence U.S.A, 2019, 6-7, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf; Jordan Fabian, "US warns of 'ongoing' election interference by Russia, China, Iran," *The Hill*, October 19, 2018, https://thehill.com/policy/national-security/412292-us-warns-of-ongoing-election-interference-by-russia-china-iran.

[9] Viriya Singgih, Arys Aditya, and Karlis Salna, "Indonesia Says Election Under Attack From Chinese, Russian Hackers," *Bloomberg*, March 13, 2019, https://www.bloomberg.com/news/articles/2019-03-12/indonesia-says-poll-under-attack-from-chinese-russian-hackers.

[10] Dean Pennington, "Australia's major parties targeted in 'sophisticated' cyber attack ahead of election," *TechSpot*, February 18, 2019, https://www.techspot.com/news/78802-australia-major-parties-targeted-ophisticated-cyber-attack-ahead.html.

[11] John V. Kelly, *Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure*, Office of Inspector General, Department of Homeland Security, February 18, 2019, https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-24-Feb19.pdf.

that the vast majority of this money is being used to strengthen election cybersecurity, purchase new voting equipment, and improve post-election audits, all essential steps that experts have agreed need immediate action.[12]

## B. There is Critical Work to be Done Ahead of the 2020 Election and Beyond

Despite this progress, there is far more work that needs to be done to improve the security of our elections in 2020 and beyond. I submit there are four main areas that deserve special attention, which I will discuss in detail below: (1) replacement of aging and insecure voting machines, particularly paperless systems, which experts agree should be removed from service as soon as possible; (2) widespread implementation of post-election audits that will provide a high level of confidence in the accuracy of the final vote tally; (3) upgrading or replacing election-related computer systems to address cyber vulnerabilities identified by DHS or similar scans or assessments of existing election systems; and (4) increased training and IT resources for state and local election officials**.** Many of these items are addressed in provisions of H.R. 1, Titles I and III, as well as other bills introduced in the last year by Republicans and Democrats.[13] Passage of these provisions would be a tremendous step forward towards securing our elections.

### 1. Many Localities Need to Replace Their Voting Machines Before 2020, and This is Particularly Urgent in States That Still Use Paperless Systems

In late 2015, the Brennan Center published *America's Voting Machines at Risk*, a comprehensive look at the voting systems used in the United States.[14] In that report, we warned of the impending crisis as voting machines around the country aged, presenting serious security and reliability challenges.

Our concern about the continued use of these systems was and is threefold. First, older systems are more likely to fail and are increasingly difficult to maintain. This was borne out in the 2018 midterm election, when old and malfunctioning voting machines across the country created long lines at the polls, leaving voters frustrated – and, in some cases, causing them to leave before casting a ballot.[15]

[12] *Grant Expenditure Report, Fiscal Year 2018*, The U.S. Election Assistance Commission, April 4, 2019, https://www.eac.gov/assets/1/6/FY2018HAVAGrantsExpenditureReport.pdf.

[13] See, e.g., For the People Act of 2019, H.R.1, 116th Cong. (2019); Election Security Act, H.R.5011, 115th Cong. (2018); Protecting the American Process for Election Results (PAPER) Act, H.R.3751, 115th Cong. (2017); Secure Elections Act, S.2261, 115th Cong. (2017).

[14] Lawrence Norden and Christopher Famighetti, *America's Voting Machines at Risk*, Brennan Center for Justice, 2015, https://www.brennancenter.org/publication/americas-voting-machines-risk.

[15] Erik Ortiz, Shamar Walters, Emily Siegel, Jareen Imam, Sarah Fitzpatrick, and Alex Johnson, "Midterms 2018: Voters face malfunctioning machines and long lines at polls across country on Election Day," *NBC News*, November 6, 2018, https://www.nbcnews.com/politics/elections/midterms-2018-voters-face-malfunctioning-machines-long-lines-polls-across-n932156; Ashley Lopez, "Old Voting Machines Confuse Some Texans During Midterm Election," *NPR*, October 30, 2018, https://www.npr.org/2018/10/30/662095109/old-voting-machines-confuse-some-texans-during-midterm-election; Christina A. Cassidy, Colleen Long, and Michael Balsamo, "Machine breakdowns, long lines mar vote on Election Day," *Associated Press*, November 6, 2018, https://www.apnews.com/6fb6de6fdb034b889d301efd12602e21; P.R. Lockhart, "Voting hours in parts of Georgia extended after technical errors create long lines," *Vox*, November 6, 2018, https://www.vox.com/policy-and-politics/2018/11/6/18068492/georgia-voting-gwinnett-fulton-county-machine-problems-midterm-election-extension.

Second, aging voting systems also use outdated hardware and software and many of them are no longer manufactured. This can make finding replacement parts difficult, if not impossible. In several cases, officials have had to turn to eBay to find critical components like dot-matrix printer ribbons, decades old memory storage devices and analog modems.[16] Aging systems also frequently rely on unsupported software, like Windows XP and 2000, which may not receive regular security patches and are thus more vulnerable to the latest methods of cyberattack.[17]

Third, older systems are less likely to have the kind of security features we expect of voting machines today. While nearly all of today's new voting machines go through a federal certification and testing program, many jurisdictions using older equipment purchased their voting machines before this process was in place. Older machines can have serious security flaws, including hacking vulnerabilities, which would be unacceptable by today's standards.

Most notably, older systems disproportionately do not employ voter-marked paper ballots that can be used to detect and recover from attacks on voting machine software. The National Academy of Sciences, Engineering, and Medicine is just one of the latest authorities to examine such systems and conclude that they should be "removed from service as soon as possible" to ensure the security and integrity of American elections.[18] They have been joined in this conclusion by the U.S. Senate Select Committee on Intelligence, as well as security experts around the country, all of whom have argued that continued use of these systems presents an unnecessary security risk.[19]

Since our 2015 report, several states have made significant progress in replacing antiquated equipment. In particular, Colorado, Michigan, Ohio and Rhode Island are among the states that have replaced all or a significant portion of their aging voting equipment. Perhaps most importantly, Virginia, Arkansas, and Delaware have completely replaced their paperless voting machines with systems that use voter-marked paper ballots, and other states, including Georgia,

[16] Mark Earley (Voting Systems Manager, Leon County, Florida) interview by Brennan Center, January 26, 2015; Paul Ziriax (Secretary, Oklahoma Board of Elections) and Pam Slater (Assistant Secretary, Oklahoma Board of Elections), interview by Brennan Center March 16, 2015; Kristin Mavromatis (Public Information Manager, Mecklenburg County, North Carolina) interview by Brennan Center, April 9, 2015. *See* Lawrence Norden and Christopher Famighetti, *America's Voting Machines at Risk*, Brennan Center for Justice, 2015, 14 , https://www.brennancenter.org/publication/americas-voting-machines-risk.

[17] For instance, Microsoft stopped supporting Windows XP in 2014, with the exception of a "highly unusual patch" that it issued in 2017 to prevent the spread of WannaCry malware. *See* Tom Warren, "Microsoft releases new Windows XP security patches, warns of state-sponsored cyberattacks," *The Verge*, June 13, 2017, https://www.theverge.com/2017/6/13/15790030/microsoft-windows-xp-vista-security-updates-june-2017.

[18] *Securing the Vote: Protecting American Democracy*, The National Academies of Sciences, Engineering, and Medicine, 2018, 5, https://www.nap.edu/read/25120/chapter/1.

[19] *Securing the Vote: Protecting American Democracy*, The National Academies of Sciences, Engineering, and Medicine, 2018, https://www.nap.edu/read/25120/chapter/1; *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations*, U.S. Senate Select Committee on Intelligence, May 8, 2018, https://www.intelligence.senate.gov/publications/russia-inquiry; Danielle Root, Liz Kennedy, Michael Sozan, and Jerry Parshall, *Election Security in All 50 States: Defending America's Elections*, Center for American Progress, February 12, 2018, https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/; "Study and Recommendations," The Blue Ribbon Commission on Pennsylvania's Election Security, 2019, 21, https://www.cyber.pitt.edu/sites/default/files/FINAL%20FULL%20PittCyber_PAs_Election_Security_Report.pdf.

Louisiana, New Jersey, South Carolina, and Pennsylvania, have taken important steps to replace this equipment.[20]

This winter, the Brennan Center surveyed election officials around the country on their need to replace their voting machines. Local officials in 31 states told us that they must replace their equipment before the 2020 election, but two-thirds of these officials said that they do not have the adequate funds to do so, even after the distribution of additional HAVA funds from Congress.[21] Meanwhile, officials in 40 states told us they are using at least some voting machines that are more than a decade old this year, perilously close to the end of the lifespan for many of these systems.[22] And officials in 45 states currently use at least some systems that are no longer manufactured, with many reporting that they have difficulty finding replacements when parts fail.[23] There should be little doubt that most of these machines will need to be replaced in the

[20] The Verifier — Polling Place Equipment — November 2018," Verified Voting, accessed February 22, 2019, https://www.verifiedvoting.org/verifier/; Delaware will start rolling out machines with paper backups on May 14 of this year. *See* Amy Cherry, "Delawareans to get 1st look at new voting machines in upcoming school board elections," *WDEL*, May 6, 2019, https://www.wdel.com/news/video-delawareans-to-get-st-look-at-new-voting-machines/article_7d625346-6ddd-11e9-a2c7-4f6dfafa74af.html; Kim Wade, "Georgia Sec. of State seeks to replace criticized voting machines," *WSAV*, January 24, 2019, https://www.wsav.com/news/local-news/georgia-sec-of-state-seeks-to-replace-criticized-voting-machines/1722859964; Mark Niesse, "Voters Confront Georgia Lawmakers Over New Touchscreen Election System," *WSB Radio*, February 19, 2019, https://www.wsbradio.com/news/state--regional-govt--politics/voters-contront-georgia-lawmakers-over-new-touchscreen-election-system/Jj26WLlCuMXKuzL6nZo9oI/; Melinda Deslatte, "Kyle Ardoin wins election for Louisiana secretary of state," *Associated Press*, December 8, 2018, https://www.apnews.com/782bb812689045328f876dd300f08840; Meghan Grant, "Some NJ voters will cast their next ballot on new, more secure voting machines," *North Jersey Record*, March 11, 2019, https://www.northjersey.com/story/news/new-jersey/2019/03/11/new-nj-voting-machine-pilots-being-rolled-out-across-state/1266947002/; Bristow Marchant, "SC takes first step toward switching to paper ballots in 2020," *The State*, January 15, 2019, https://www.thestate.com/news/politics-government/article224557350.html; Marc Levy, "Pennsylvania must replace voting machines, lawmakers told," *AP News*, February 20, 2019, https://www.apnews.com/15e507d74d0e439faf775cc45bb0aa7d.

[21] In our survey, election officials in 31 states (Arizona, Arkansas, California, Colorado, Delaware, Florida, Georgia, Illinois, Iowa, Kansas, Maine, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Nebraska, New Hampshire, New York, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, West Virginia, Wisconsin, and Wyoming) told us they needed to replace their voting machines by 2020. *See* Lawrence Norden and Andrea Córdova, "Voting Machines at Risk: Where We Stand Today," *Brennan Center for Justice*, March 5, 2019, https://www.brennancenter.org/analysis/voting-machines-risk-where-we-stand-today.

[22] In our survey, jurisdictions from 40 states (Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Maine, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New Mexico, New York, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming) told us that their voting machines were at least a decade old. *See* Lawrence Norden and Andrea Córdova, "Voting Machines at Risk: Where We Stand Today," *Brennan Center for Justice*, March 5, 2019, https://www.brennancenter.org/analysis/voting-machines-risk-where-we-stand-today.

[23] The Brennan Center confirmed with three major vendors (ES&S, Dominion, and Hart InterCivic) that the following models are no longer manufactured: iVotronic, M100, M650, AutoMark (ES&S); AccuVote OS, AccuVote OSX, AccuVote TS, AccuVote TSX, AVC Edge, AVC Advantage, Optech IIIP-Eagle and Optech Insight (Dominion); eScan, eSlate and Judge's Booth Controller (Hart Intercivic). Danaher's Shouptronic 1242, used mainly in Delaware, is also no longer manufactured. We used this information to confirm that seven states (Delaware, Georgia, Hawaii, Louisiana, North Dakota, Oklahoma, and South Carolina) are using exclusively discontinued voting machines, 38 states (Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Florida, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Massachusetts, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New York, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming) use

coming years.

Nearly 100 percent of election officials who hoped to replace their machines before 2020 stated that they intend to replace their systems with machines that produced a voter-verifiable paper record that could be used to detect and recover from an attack on voting system software. And yet, while several states have passed laws or taken steps to replace paperless voting machines before 2020, most have not yet secured sufficient funds for local election officials to do so. Today, 11 states still use paperless electronic machines as the primary polling place equipment in at least some counties and towns (Georgia, Indiana, Kansas, Kentucky, Louisiana, Mississippi, New Jersey, Pennsylvania, South Carolina, Tennessee and Texas). Three (Georgia, Louisiana, and South Carolina) continue to use such systems statewide.[24]

The Brennan Center has estimated it would cost more than $300 million to replace all remaining paperless voting machines in the United States and more than $700 million to replace voting machines that are currently over a decade old.[25]

### 2. More States Should Conduct Robust Post-Election Audits

As the Brennan Center noted in its 2006 report *The Machinery of Democracy*, moving to paper-based systems without using the paper to check the accuracy of electronic totals may be of “limited security value.”[26] Paper records will not prevent programming errors, software bugs, or the insertion of corrupt software into voting systems. Voter-marked paper ballots will only have real security value if they are used to check and confirm electronic tallies.[27]

Since the issuance of that report, we have made tremendous strides in developing post-election audits that can efficiently allow us to detect and recover from a software hack or bug that could alter an election outcome. In particular, post-election risk-limiting audits (RLAs) require hand

discontinued voting machines in one or more jurisdictions, and five states (Maine, Maryland, Michigan, Nevada, New Mexico) and the District of Columbia use machines that are all currently manufactured. See Kathy Rogers, (Senior Vice President of Government Relations, ES&S), Conversation with Edgardo Cortez, February 13, 2019; Kay Stimson (Vice President, Government Affairs, Dominion), Email message to Edgardo Cortez, Feb 27, 2019; Sam Derheimer (Director of Government Affairs, Hart InterCivic), Email message to Edgardo Cortez, Feb 14, 2019; “Danaher Shouptronic 1242,” Verified Voting, accessed February 25, 2019, https://www.verifiedvoting.org/resources/voting-equipment/danaher/shouptronic/; “The Verifier — Polling Place Equipment — November 2018,” Verified Voting, accessed February 25, 2019, https://www.verifiedvoting.org/verifier/.

[24] “The Verifier — Polling Place Equipment — November 2018,” Verified Voting, accessed May 6, 2019, https://www.verifiedvoting.org/verifier/.

[25] “Estimate for the Cost of Replacing Paperless, Computerized Voting Machines,” Brennan Center for Justice, 2018, https://www.brennancenter.org/sites/default/files/analysis/New_Machines_Cost_Across_Paperless_Jurisdictions%20%282%29.pdf; Relying on Verified Voting data from November 2018, we estimated that 90,140 precincts are using voting machines that are at least 10 years old. We multiplied this number of precincts by $8,000, our estimate for per-precinct machine replacement cost, to arrive to our $700 million estimate.

[26] Lawrence Norden, *The Machinery of Democracy: Protecting Elections In An Electronic World*, Brennan Center for Justice, 2006, https://www.brennancenter.org/sites/default/files/publications/Machinery%20of%20Democracy.pdf.

[27] Ibid.

counts of statistical samples of voter verifiable paper ballots. In the words of the EAC, such audits provide "strong statistical evidence that the election outcome is right and has a high probability of correcting a wrong outcome,"[28] and are thus a critical measure for increasing the public confidence in and integrity of our elections.

Unfortunately, only 22 states that have paper records of every vote require post-election audits of those votes before certifying their elections.[29] This is only two more than did so in 2016.[30] Even in states where post-election audits are required, in most cases they could be far more robust; only two, Colorado and Rhode Island, will require RLAs in 2020.

Still, it is clear that more jurisdictions are hoping to expand the use of RLAs. Three additional states—California, Ohio, and Washington—allow election officials to select them from a list of audit types.[31] Georgia recently passed a law that would require RLAs beginning in 2021.[32] Bills to require RLAs or authorize RLA pilots are also pending in New York, Indiana, South Carolina, and New Jersey.[33] Several more jurisdictions have recently piloted these post-election audits, and even more intend do so in 2019. This includes election jurisdictions in Michigan, New Jersey, Rhode Island, Virginia, Indiana and California.[34] A number of these jurisdictions used the 2018 Congressional HAVA grants to conduct the pilots.[35]

[28] Jerome Lovato, "Defining and Piloting Risk-Limiting Audits," *U.S. Election Assistance Commission*, accessed May 6, 2019, https://www.eac.gov/defining-and-piloting-risk-limiting-audits-/.

[29] These twenty-two states are Alaska, Arizona, California, Colorado, Connecticut, Hawaii, Illinois, Iowa, Massachusetts, Minnesota, Missouri, Montana, Nevada, New Mexico, New York, North Carolina, Ohio, Oregon, Rhode Island, Utah, Washington, and West Virginia. Although Ohio conducts post-election audits after certification, the Election Board must amend its certification if the audit results in a change of the vote totals reported in the official canvass; *See* "POST-ELECTION AUDITS," National Conference of State Legislatures, last modified February, 1, 2019, accessed May 6, 2019, http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx ; Danielle Root, Liz Kennedy, Michael Sozan, and Jerry Parshall, *Election Security in All 50 States: Defending America's Elections*, Center for American Progress, February 12, 2018, https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/.

[30]17 R.I. Gen Laws §17-19-37.4 (2017); 2017 Iowa Acts 256.

[31] *CAL. ELEC CODE* §15365-15367*; Ohio Election Official Manual*, Ohio Secretary of State, August 1, 2018, https://www.sos.state.oh.us/globalassets/elections/directives/2017/dir2017-10_eom.pdf/; WASH. REV. CODE ANN. §29A.60.185.

[32] H.B 316, 2019 Gen. Assemb., Reg. Sess. (Ga. 2019).

[33] S.B. 2329, 2019 Leg., Reg. Sess. (Ny. 2019); S.B. 405, 121st Gen. Assemb., Reg. Sess. (In. 2019); H.B 3304, 2019 Gen. Assemb. 123rd Sess. (Sc. 2019); A.B. 3991, 218th Leg., (Nj. 2018).

[34] Kellie Ottoboni, "Piloting Risk-Limiting Audits in Michigan," *Berkeley Institute for Data Science*, December 20, 2018, https://bids.berkeley.edu/news/piloting-risk-limiting-audits-michigan; Abigail Abrams, "Russia Wants to Undermine Trust in Elections. Here's How Rhode Island Is Fighting Back," *Time Magazine*, January 26, 2019, http://time.com/5510100/risk-limiting-audit-election-security/; *Risk-Limiting Audits,* Department of Elections, Virginia, September 20, 2018, https://www.elections.virginia.gov/media/Media/Agendas/2018/20180920-RLA_Report.pdf; Stephanie Singer and Neal McBurnett, *Orange County, CA Pilot Risk-Limiting Audit*, Verified Voting, December 7, 2018, https://www.verifiedvoting.org/wp-content/uploads/2018/12/2018-RLA-Report-Orange-County-CA.pdf.

[35] Abigail Abrams, "Russia Wants to Undermine Trust in Elections. Here's How Rhode Island Is Fighting Back," *Time Magazine*, January 26, 2019, http://time.com/5510100/risk-limiting-audit-election-security/ Colleen O'Dea, "Progress seen in test of paper-trail voting machines that allow audit of results," *NJ Spotlight*, January 4, 2019, https://www.njspotlight.com/stories/19/01/03/progress-seen-in-test-of-paper-trail-voting-machines-that-allow-audit-of-results/.

The Brennan Center has strongly encouraged all states to adopt robust post-election audits. More pilots of RLAs, in particular, will help to get us to a point where we can conduct these nationwide and have a high level of confidence that a software bug, error, or hack did not change the outcomes of federal contests. We believe Congress should take steps to encourage states and localities to adopt this critical security measure.

### 3. States and Counties Must Upgrade or Replace Election-Related Computer Systems and Websites Where Vulnerabilities are Discovered

The Special Counsel's Report makes clear that there is a much larger infrastructure than just voting machines that we need to protect from cyberattack. Indeed, if we look at incursions into election systems in the United States and abroad over the last few years, including since 2016, we see some of the most common targets are election officials' e-mail, state and locality voter registration databases, election night reporting, and other election websites.[36]

At least 21 states have requested Risk and Vulnerability Assessments of their election-related networks and computer systems from DHS, and several additional states have contracts with private vendors to conduct assessments of the entirety of their election-related computer systems.[37] The Brennan Center has advocated that all states implement a process of continuous cybersecurity vulnerability assessments. While we estimate the cost of such assessments will be no more than a few million dollars annually, the cost of securing vulnerabilities identified by such assessments is likely to cost many millions more.[38]

Without question, one of the most important and costly sets of systems to secure – through upgrades or replacements – will be state and local voter registration databases. Indeed, many registration systems in the United States are as old as or older than voting systems in use today. If anything, the use of outdated databases and operating systems presents even more challenges than those associated with using old voting machines. As Marc Burris, Chief Information Officer of the North Carolina State Board of Elections put it, at least the oldest voting machines in the

[36] Pavel Polityuk, "Exclusive: Ukraine says it sees surge in cyber-attacks targeting election," *Reuters*, January 25, 2019, https://www.reuters.com/article/us-ukraine-cyber-exclusive/exclusive-ukraine-says-it-sees-surge-in-cyber-attacks-targeting-election-idUSKCN1PJ1KX; Viriya Singgih, Arys Aditya, and Karlis Salna, "Indonesia Says Election Under Attack From Chinese, Russian Hackers," *Bloomberg*, March 13, 2019, https://www.bloomberg.com/news/articles/2019-03-12/indonesia-says-poll-under-attack-from-chinese-russian-hackers; Benjamin Wofford, "The hacking threat to the midterms is huge. And technology won't protect us," *Vox*, October 25, 2018, https://www.vox.com/2018/10/25/18001684/2018-midterms-hacked-russia-election-security-voting; Lynn Sweet, "Mueller report confirms Russians 'compromised' Illinois State Board of Elections," *Vox*, April 18, 2019, https://chicago.suntimes.com/news/mueller-report-special-counsel-russia-hacking-illinois-state-board-elections/.

[37] Chris Good, "Fewer than half of US states have undergone federal election security reviews ahead of midterms," *ABC News*, October 30, 2018, https://abcnews.go.com/Politics/fewer-half-us-states-undergone-federal-election-security/story?id=58858453.

[38] Matt Damschroder, (Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio), in phone discussion with Lawrence Norden; Edgardo Cortes (Commissioner, Department of Elections, Virginia), email message to Lawrence Norden, June 20, 2017, *See* Lawrence Norden and Ian Vandewalker, *Securing Elections from Foreign Interference*, Brennan Center for Justice, 2017, 19, https://www.brennancenter.org/publication/securing-elections-foreign-interference; Robert A. Brehm (Co-Executive Director, New York State Board of Elections), interview by Brennan Center for Justice, May 6, 2019; Mandy Vigil (Acting Elections Director, New Mexico Secretary of State), interview by Brennan Center for Justice, May 6, 2019.

United States were actually "designed for a longer shelf life. That's not true of many of the database systems we are using today."[39]

In September 2015, the Brennan Center estimated that 41 states were using voter registration databases that were initially created at least a decade ago. While some states have since replaced or substantially upgraded their systems, most have not.[40] In the past decade, of course, cyber threats have advanced enormously. As Edgardo Cortés, former Commissioner for the Virginia Department of Elections and Brennan Center Election Security Advisor, has noted, "These systems weren't designed with [current cyber threats] in mind." Officials from a number of states, including Arizona, Minnesota, New Jersey, and Pennsylvania, have stated that they hope to invest in improving or replacing their voter registration systems in the very near future.

The need for updates or replacement of IT infrastructure and software may be even greater at the local level, where systems often run on discontinued software like Windows XP or Windows 2000 that is more vulnerable to cyberattack because it is no longer vendor supported. This is particularly troubling because smaller jurisdictions frequently have little or no IT support of their own. As Matt Damschroder (former Assistant Secretary of State in Ohio) has noted, "at the state level, you are generally going to have more resources and higher levels of sophistication."[41] Local election officials are likely to have "far fewer resources" to protect against attacks.

### 4. Local Election Jurisdictions Need More Cybersecurity Resources

The vast and decentralized election system in the United States means our elections are largely run at the local level. While there are certainly security benefits associated with this decentralization,[42] there are also obvious risks. Foremost among these is the fact that with over 8,000 separate election offices, there are many potential targets. As Bob Brehm, Co-Executive Director of the New York State Board of Elections, recently put it in an interview with the Brennan Center, "it is not reasonable" to expect each of these state and local election offices to independently "defend against hostile nation-state actors."[43] This is particularly true in the case of local election offices that frequently have little or no in-house IT or cybersecurity resources.

[39] Marc Burris (IT Director and CIO, State Board of Elections, North Carolina), in phone discussion with Lawrence Norden, May 22, 2017, *See* Lawrence Norden and Ian Vandewalker, *Securing Elections from Foreign Interference*, Brennan Center for Justice, 2017, 19, https://www.brennancenter.org/publication/securing-elections-foreign-interference.

[40] "California Secretary of State Certifies Centralized Statewide Voter Registration System," *Government Technology*, September 28, 2016, https://www.govtech.com/computing/California-Secretary-of-State-Certifies-Centralized-Statewide-Voter-Registration-System.html; "In November of 2017, a contract was issued to Sutherland Government Solutions, Inc. for the acquisition of a new statewide voter registration database ("AVID") that will replace our currently aging system ("VRAZII") on or before June 30, 2019," *See Arizona: 2018 HAVA Election Security Funds*, Arizona Secretary of State, 2018, 2, https://www.eac.gov/havadocuments/AZ_Narrative_Budget.pdf.

[41] Matt Damschroder, (Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio), in phone discussion with Lawrence Norden, *See* Lawrence Norden and Ian Vandewalker, *Securing Elections from Foreign Interference*, Brennan Center for Justice, 2017, 20, https://www.brennancenter.org/publication/securing-elections-foreign-interference.

[42] *See* Dr. Dan S. Wallach, Testimony Before the House Committee on Space, Science & Technology Hearing 4, September, 13, 2016, https://www.cs.rice.edu/~dwallach/pub/us-house-sst-voting-13sept2016.pdf.

[43] Robert A. Brehm (Co-Executive Director, New York State Board of Elections), interview by Brennan Center for Justice, May 6, 2019.

I want to highlight two steps that states have already taken which, if adopted nationally, could bring greater cybersecurity protection to our local election offices. The first is the creation of statewide "cyber navigator" or cyber liaison programs for local election offices. As DHS has noted, "the purpose of these navigators is to provide practical cybersecurity knowledge, support and services to local election officials who otherwise would not have them."[44]

The state of Illinois recently allocated at least $7 million to create a cyber navigator program for its local election offices. Among other things, this money will be used to support 9 cyber navigators, assigned to geographic zones, who go into county clerks' offices to conduct trainings, risk assessments and evaluations to determine what type of equipment and software upgrades will be necessary, as well as to serve as a resource for county election offices going forward.

Illinois was able to use much of the HAVA funding it received in 2018 to launch its cyber navigator program. Other states like Alaska, Arkansas, Delaware, Louisiana, and Pennsylvania, which had to use their funds toward replacement of their paperless voting machines, will not have the luxury of using those funds for these purposes.

New York has chosen to use their HAVA funds to purchase intrusion detection services for all county election offices. New York State is spending $5 million to provide these services to all counties that were not provided with them for free under a program offered by the Elections Infrastructure Sharing Analysis Center (EI-ISAC) run by Center for Internet Security with support from DHS.[45] In interviews by the Brennan Center with local election officials, the desire for these kind of detection services has come up repeatedly.[46]

### C. Congress Has a Critical Role to Play as Partner and Leader

Congress has a critical role to play, both in partnering with states and local governments by funding needed security steps, and providing direction about how that federal money should be used. As Michael Chertoff and Grover Norquist have put it, "Congress should recognize that election cybersecurity reforms are in their own personal interest – and in the interest of the United States national security."[47]

[44] *DHS Election Infrastructure Security Funding Consideration*, National Protection and Programs Directorate Department of Homeland Security, June 13, 2018, 2, https://www.dhs.gov/sites/default/files/publications/Election%20Infrastructure%20Security%20Funding%20Considerations%20Final.pdf.

[45] Robert A. Brehm (Co-Executive Director, New York State Board of Elections), interview by Brennan Center for Justice, May 6, 2019.

[46] Dana Debeauvoir (County Clerk, Travis County, Texas), interview by Brennan Center for Justice, February 14, 2019. *See* Lawrence Norden and Andrea Córdova, "Voting Machines at Risk: Where We Stand Today," *Brennan Center for Justice*, March 5, 2019, https://www.brennancenter.org/analysis/voting-machines-risk-where-we-stand-today.

[47] Michael Chertoff and Grover Norquist, "We need to hack-proof our elections. An old technology can help," *The 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=.bfeb06fa4a86.

Funding elections should be a shared responsibility at the local, state, and federal level, but only Congress has the power to ensure that responsibility is shared by providing grants that must be matched by state and local governments. Obvious first steps for such money should include the items touched on in my testimony today, including replacing paperless voting machines before 2020 and conducting robust post-election audits.

Congress should also share in longer-term funding for things like regular risk assessments and necessary repairs and upgrades for critical infrastructure, as well as grants for cybersecurity resources that are directed to local election offices, which are frequently under-resourced relative to their state counterparts.

Finally, Congress should consider what additional steps it can take to protect our election infrastructure from attacks against private election system vendors, who were targeted in 2016 and are likely to be targeted again. Private companies perform every duty from building and maintaining election websites that help voters determine how to register and where they can vote, to printing and designing ballots, to programming voting machines before each election, to building and maintaining voter registration databases, voting machines, and electronic pollbooks. To be sure, not every jurisdiction outsources all these functions, but all rely on private vendors for some of this work and many for all of it.

And yet, in contrast to other sectors, particularly those that the federal government has designated "critical infrastructure," there is almost no federal oversight of private vendors that design and maintain the systems that allow us to determine who can vote, how they vote, what voters see when they cast their vote, how votes are counted and how those vote totals are communicated to the public. In fact, there are more federal regulations for ballpoint pens and magic markers than there are for voting systems and other parts of our federal election infrastructure.[48]

One important step would be to mandate that vendors report any cyber security incident they discover to both the federal authorities as well as state and local customers. Reporting of cyber security incidents for election vendors may seem like a small step, but it will have a large impact on the overall security position of election officials around the country. Election vendors have stated that such requirements are unnecessary and burdensome and that they are somehow different from the vendors in other critical infrastructure sectors. This is simply not true. We know that the lack of transparency in vendor security is a significant vulnerability to election security. In fact, reporting requirements for cyber security incidents are a bare minimum, and we should be considering additional requirements such as vendor employee background checks and other lessons learned from other critical infrastructure sectors.[49] The Brennan Center has documented some of the additional reasons for mandating such reporting in the 2010 report, *Voting System Failures: A Database Solution*.[50]

[48] Compare, for example, 16 C.F.R. §§ 1500.14, 1500.48, 1500.83, 1700.14, with 11 CFR §§ 9405.1 et seq.

[49] Brian Calkin, Kelvin Coleman, Brian de Vallance, Thomas Duffy, Curtis Dukes, Mike Garcia, John Gilligan, Paul Harrington, Caroline Hymel, Philippe Langlois, Adam Montville, Tony Sager, Ben Spear, Roisin, *A Handbook for Elections Infrastructure Security*, Center for Internet Security, February 2018, https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf.

[50] Lawrence Norden, *Voting System Failures: A Database Solution*, Brennan Center for Justice, 2010, https://www.brennancenter.org/publication/voting-system-failures-database-solution.

## D. Conclusion

America has made great progress since 2016 in securing our elections. But in an era when hostile nation powers are likely to continue to see American election infrastructure as a target, we cannot rest on our laurels. As one election official noted in an interview with the Brennan Center, "we are trying to build the [protective] wall faster than our opponents are tearing it down."[51] Doing so requires consistent, coordinated resources and leadership from all levels, including Congress, federal agencies, the states, and local governments.

[51] Kathy Boockvar (Acting Secretary of the Commonwealth, Pennsylvania), interview by Brennan Center for Justice, May 3, 2019.