Committee on Homeland Security
United States House of Representatives

Statement of Elizabeth L. Howard
Counsel, Democracy Program
Brennan Center for Justice at NYU School of Law
October 15, 2019

"Preparing for 2020: How Illinois is Securing Elections"

Chairman Thompson, Ranking Member Rogers, 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 our analysis of the important efforts to secure election systems in Illinois and across the country based on the results of our extensive studies and work to ensure our nation's election systems are more secure and reliable across the country. We are deeply involved in the effort to ensure accurate and fair voting for all Americans.

For over a decade, I have worked on election administration issues. In my former position as Deputy Commissioner of Elections in Virginia, I coordinated various election security projects, including the decertification of all paperless voting machines in 2017. In my current role, I focus almost exclusively on election security. Representing the Brennan Center, I frequently partner with state and local election officials to assist with the implementation of important election security measures and serve on the Michigan Secretary of State's Election Security Commission and the Pennsylvania Secretary of State's Audit Working Group. I have also co-authored multiple reports on election security and remedial measures and policies that will better enable our election infrastructure to withstand attack.

Most recently, I co-authored Defending Elections, which demonstrates the need for additional election security resources across the country. This report includes detailed profiles of recent election security efforts and ongoing needs in six states, including Illinois. We noted that as part of Russia's "sweeping and systemic" efforts to interfere with our elections in 2016, Russian operatives "compromised the computer network of the Illinois State Board of Elections . . . [,] then gained access to a database containing information on millions of registered Illinois voters, and extracted data related to thousands of U.S. voters before the malicious activity was identified."[1] And, although there is no panacea to counter such threats, Illinois has implemented a variety of election security measures which should help identify and patch or otherwise address cybersecurity vulnerabilities like those the Russians exploited in 2016.

Based on our extensive election security studies and partnerships with a diverse range of election officials, we believe that Illinois's successes and struggles in its ongoing effort to secure the state's election infrastructure are instructive when analyzing the election security landscape across the country. In Illinois, and across the country, there has been much progress since 2016, but much work remains to be done.

I hope to convey three points in my testimony today:

(1) The risks facing our nation's election infrastructure in 2020 require urgent action;
(2) Illinois has taken many important steps to improve election security, including implementation of a cyber navigator program, but there is more to do; and
(3) Congress has a critical leadership and partnership role to play in helping Illinois and other states ensure our elections are free, fair and secure.

A. The risks facing our election infrastructure must be urgently addressed.

Illinois was not the only state targeted by Russia in 2016. We now know that Russia likely targeted state and local election boards in all 50 states and used spear phishing attacks to gain access to and infect computers of a voting technology company and two Florida counties.[2] We also know there is good reason to believe we face even more serious threats in 2020 and beyond. 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.

In many ways, the major cybersecurity risks posed today by Russia and other hostile foreign nation states are not new. They include hacking, e.g., SQL injections and ransomware attacks,

[1] Christopher R. Deluzio, Liz Howard, Paul Rosenzweig, David Salvo, and Rachael Dean Wilson, *Defending Elections*, Brennan Center for Justice, 2019, https://www.brennancenter.org/sites/default/files/publications/2019_07_EACFunding%20Report_FINAL.pdf.

[2] *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1*, Senate Select Committee on Intelligence, 2019, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf ("DHS assessed that the searches, done alphabetically, probably included all 50 states, and consisted of research on "general election-related web pages, voter ID information, election system software, and election service companies."); Miles Parks, "Florida Governor Says Russian Hackers Breached 2 Counties In 2016," *NPR*, May 14, 2019, https://www.npr.org/2019/05/14/723215498/florida-governor-says-russian-hackers-breached-two-florida-counties-in-2016; Sean Gallagher, "DHS, FBI say election systems in all 50 states were targeted in 2016," Ars Technica, April 10, 2019, https://arstechnica.com/information-technology/2019/04/dhs-fbi-say-election-systems-in-50-states-were-targeted-in-2016/ ("The FBI and DHS assess that Russian government cyber actors probably conducted research and reconnaissance against all US states' election networks leading up to the 2016 Presidential elections."); Election Security Hearing, Before the Comm. on House Administration, 116th Cong. (2019) (statement of Lawrence Norden).

distributed denial of service (DDoS) attacks and insider threats.[3] Like other government officials responsible for protecting the integrity of IT systems and the information they maintain, election officials are struggling to manage these risks.[4]

Election officials hold a special place in our democracy. Not only are they responsible for protecting our election infrastructure, but also maintaining and bolstering confidence in the democratic process we use to decide who will serve important governmental roles at the federal, state and local level. Americans' faith in the integrity of this system is the foundation of our ability to self-govern and is in peril.[5]

Election officials should not be tasked with shouldering this responsibility alone. Under our federal system of government, the risks facing individual election jurisdictions are a threat to every American who has confidence in our democracy. Successful attacks against our infrastructure in any county in any state can have a ripple effect that impacts the balance of power at the federal level. While the decentralized nature of our electoral system is a strength in many ways, we are only as strong as our weakest link.

There is widespread agreement on many of the remedial measures and policies necessary to create a resilient election infrastructure. We urge Congress to take immediate steps to protect the votes cast by every American by passing common-sense legislation to ensure implementation of minimum election security standards across our nation and by paying its fair share of the associated costs.

B. Illinois officials have implemented many important election security measures and policies, including a cyber navigator program, but much work remains to be done at the federal and state level to address significant security gaps.

In the wake of Russia's successful infiltration of Illinois' voter registration database in 2016, Illinois officials took prompt action to address identified vulnerabilities. Their work continues today. Illinois' ongoing efforts to further strengthen their election infrastructure include

[3] Meredith Berger et al., *The State and Local Election Cybersecurity Playbook*, Harvard Kennedy School and Defending Digital Democracy, 2018, https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf.

[4] See e.g., Kylie Bielby, "GAO: Federal Agencies Struggle to Manage Cybersecurity Risks," Homeland Security Today, July 26, 2019, https://www.hstoday.us/exclude-from-homepage/gao-federal-agencies-struggle-to-manage-cybersecurity-risks/; Alyza Sebenius and Kartikay Mehrotra, "States Struggle to Update Election Systems for 2020," *Bloomberg*, August 15 2019, https://www.bloomberg.com/news/articles/2019-08-15/states-struggle-to-update-election-systems-ahead-of-2020; 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; Kate Rabinowitz, "Election Security a High Priority — Until It Comes to Paying for New Voting Machines," *ProPublica*, February 20, 2018, https://www.propublica.org/article/election-security-a-high-priority-until-it-comes-to-paying-for-new-voting-machines.

[5] Robert S. Mueller III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, U.S. Department of Justice, 2019, https://www.justice.gov/storage/report.pdf (characterizing the Russian government's interferences as a "sweeping and systematic" effort to undermine faith in our democracy).

welcoming public and private election security partners, such as the U.S. Department of Homeland Security (DHS), and taking advantage of a wide range of free resources available.

In addition, they are using the entirety of the state's 2018 federal election security grant funds, approximately $14 million, for cybersecurity improvements. The hallmark of that effort is the state's cyber navigator program; the state plans to devote at least half of its federal grant toward this program. While much progress has been made in Illinois, the 2018 grant funds were simply not enough to address all the state's critical election security needs. In fact, the federal grant funds were similarly insufficient in every state leaving election officials across the country in a grim situation. They were forced to decide which critical election security projects to fund – and which not to. In Illinois, this meant no federal funding was available for urgent needs such as replacing antiquated voting equipment.

Illinois' Cyber Navigator Program Addresses a Critical Election Security Need and Serves as a Model for Other States Across the Country.

In 2018, Illinois launched its cyber navigator program (CNP). As part of this program, cyber navigators with responsibility for geographic zones across the state work with local election officials to train relevant personnel and to lead risk assessments and evaluations, among other things. They fill a role akin in many ways to that of a chief information security officer for counties. Their assessment and evaluation efforts help officials identify vulnerabilities and determine where additional resources may be needed to shore up cyber defenses. The program's other principal components are infrastructure improvement, through the Illinois Century Network Expansion, and information sharing, through the Cybersecurity Information Sharing Program.[6]

This program addresses a critical problem facing many local election officials in Illinois and across the country: the lack of IT and cybersecurity support at the local level.[7] Without a state resource for cyber assistance, local election officials who do not have dedicated IT staff may be at greater risk of a successful cyberattack. These officials may not have sufficient resources to appropriately respond to identified cyber threats to local systems or equipment, such as those risks shared by the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).

Federal, state and local officials across the country and the Brennan Center support the widespread adoption of this program,[8] which has been identified as an important component of Illinois' comprehensive approach to securing the state's election infrastructure.

[6] Deluzio et al., *Defending Elections*.

[7] Deluzio et al., *Defending Elections*.

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

i. Most of Illinois' Voting Machines are Antiquated and Many Do Not Use Paper Ballots. They Must Be Replaced and Robust-Post Audits Must Be Implemented.

Millions of Illinois voters will go to the polls to cast their ballot on Election Day 2020. They will encounter a variety of different voting machines at their polling place, from hand-marked paper ballot systems in some counties to antiquated Direct Recording Electronic (DRE) machines that produce a voter-verifiable paper audit trail (VVPAT) in others. As "the bulk of the voting machinery in Illinois is at least 15 years old,"[9] the ongoing use of these machines expose voters to multiple security risks.

First, aging voting systems, in general, are a security risk and less reliable than voting equipment available today. Older systems are "more likely to fail and are increasingly difficult to maintain."[10] Many used in Illinois, such as the AccuVote TSX used in multiple Illinois counties, including DuPage County, are no longer manufactured so finding replacement parts will be increasingly difficult over time.[11] This problem exacerbates the reported system-specific security concerns with other older systems used in Illinois, such as the AutoMARK, including inconsistent vote tallying and reboot times of 15 to 20 minutes.[12] Moreover, these systems simply lack important security features expected of voting machines today, such as hardware access deterrents for ports.[13]

The continued use of antiquated equipment is a concern in many other states as well. We estimate at least some voters in as many as 38 states will cast their 2020 ballot on equipment that is more than 10 years old.[14] In November 2018, we estimate that 34 percent of all local election

[9] Rick Pearson, "Illinois Pushes Millions Toward Securing Its Election Systems," *Government Technology*, August 5, 2019, https://www.govtech.com/budget-finance/Illinois-Pushes-Millions-Toward-Securing-Its-Election-Systems.html.

[10] Election Security Hearing, Before the Comm. on House Administration, 116th Cong. (2019) (statement of Lawrence Norden); Josie Bahnke (Elections Director, Office of the Lieutenant Governor, Alaska), Letter to Election Policy Work Group Members, July 18, 2018, http://www.elections.alaska.gov/doc/info/180718%20EPWG%20Research.pdf ("Today the DOE is at a critical juncture: Alaska's voting equipment and technology are outdated, difficult to repair and prone to failure.").

[11] Lawrence Norden and Andrea Cordova, "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.

[12] Ruth Johnson (Oakland County clerk/register of deeds), Letter to Rosemary Rodriguez (chairperson, Election Assistance Commission), October 2, 2008, https://www.eac.gov/assets/1/6/Oakland_County_Michigan_letter_regarding_ES_S_M-100_voting_machine_tabulators.pdf (stating that 8 percent of M-100 fleet in Oakland County "reported inconsistent vote totals during their logic and accuracy testing"); "Election Systems and Software (ES&S) AutoMARK," Verified Voting, accessed May 4, 2019, https://www.verifiedvoting.org/resources/voting-equipment/%20ess/automark/ (listing AutoMARK security concerns).

[13] Deluzio et al., *Defending Elections*.

[14] Norden and Cordova, "Voting Machine Security" (Forty-one states minus Alaska, California, and North Dakota).

jurisdictions were using voting machines that were at least 10 years old as their primary polling place equipment (or as their primary tabulation equipment in all vote-by-mail jurisdictions).[15] Next, although VVPATs were "designed primarily for audit purposes," studies have found they have some significant shortcomings.[16] For example, one report examining VVPATs in Cuyahoga County, OH found almost 10% of the VVPAT tapes "were either destroyed, blank, illegible, missing, taped together or otherwise compromised," and 19% of the tapes indicated discrepancies with the reported counts.[17] Auditing VVPATs also takes more time than auditing paper ballots "due to the need to physically separate the ballots from the spool in the first count."[18] Finally, the results of least one study "suggest that people count optical scan ballots somewhat more accurately than VVPAT paper tapes."

Cybersecurity experts, including the National Academies of Sciences, Engineering and Medicine, agree that DREs with VVPAT represent a security risk and elections should be conducted using human-readable paper ballots.[19] The U.S. House of Representatives recently indicated its support for replacement of all DREs by voting to provide $600 million in election security funding to states and requiring those states that continue to use DREs to first use these funds to replace them.[20]

[15] Ibid.

[16] Stephen N. Goggin et al., "Comparing the Auditability of Optical Scan, Voter Verified Paper Audit Trail (VVPAT) and Video (VVVAT) Ballot Systems," *USENIX The Advanced Computing Systems Association*, 2008, https://www.usenix.org/legacy/events/evt08/tech/full_papers/goggin/goggin.pdf ("While VVPAT and VVVAT systems are both designed primarily for audit purposes, the actual implementation of VVPAT auditing has not been free from problems. For example, the Election Science Institute (ESI) examined all aspects of election administration in Cuyahoga County, Ohio during the May 2006 primary election. The ESI report found that 10% of VVPAT spools were unreadable or missing, while 19% of the spools indicated discrepancies with the reported counts (ESI, 2006). Alternatives like VVVAT systems are still currently under development.")

[17] *DRE Analysis for May 2006 Primary: Cuyahoga County, Ohio*, Election Science Institute, August 2006, 6, https://web.archive.org/web/20120330212509/http://votingindustry.com/TabulationVendors/1stTier/Diebold/esi_cuyahoga_final.pdf.

[18] Stephen N. Goggin et al., "Comparing the Auditability of Optical Scan…"; see also Joseph Hall, "McCormack Hit Job Video on VVPAT," *Not Quite a Blog*, March, 23, 2019, https://josephhall.org/nqb2/index.php/mccormack_vvpat_vid ("Recounting VVPAT ballots cast during early voting on DREs in conjunction with the pilot program ran for the November 2002 election in Sacramento County, California proved even more labor intensive. Sacramento County Registrar of Voters Jill LaVine, in Congressional testimony on July 7, 2004 reported **the recount of 114 VVPAT ballots took 127 hours, approximately 1 hour per ballot due to the complexity of the long ballot for that election.").

[19] *Securing the Vote*, The National Academies of Sciences, Engineering, and Medicine, 2018, https://www.nap.edu/read/25120/chapter/1 ("Electronic voting systems that do not produce a human-readable paper ballot of record raise security and verifiability concerns.")

[20] Financial Services and General Government Appropriations Bill 2020 Report, House Committee on Appropriations, 2019, 3, 51-52, 112, https://docs.house.gov/meetings/AP/AP00/20190611/109632/HMKP-116-AP00-20190611-SD003.pdf.

Illinois is one of only a small number of states that continue to use DREs with VVPATs as the primary voting system in one or more jurisdictions.[21] In 2020, Illinois may be one of as few as 7 states with counties that rely primarily on these machines.[22] The ongoing use of DREs with VVPATs makes the current election infrastructure in Illinois slightly more secure than the infrastructure in the eight states (Indiana, Kansas, Kentucky Louisiana, Mississippi, New Jersey, Tennessee, & Texas) we estimate will use paperless DREs in 2020.

DREs with VVPATs are more secure than paperless DREs because the VVPAT can be audited after the election. Unlike some states, Illinois does take advantage of this security feature by conducting an audit of these paper records to check and confirm electronic vote tallies. We estimate that Illinois will be one of only 24 states and the District of Columbia that will have voter verifiable paper records for all votes cast and require post-election audits of those paper records before certifying election results in 2020.[23]

Illinois relies on the traditional post-election audit method, in which the results from voting equipment in a specific percentage of precincts are reviewed. This method provides assurance that individual voting machines are correctly tabulating votes. Risk-limiting audits (RLAs) are a relatively new type of audit that provide assurance that election *outcomes* are correct by using statistics to analyze random samples of all votes cast. In 2020, RLAs will be required statewide in Colorado and Rhode Island and may be conducted in lieu of traditional post-election audits at the county level in California, Ohio and Washington.

The Brennan Center has long supported both a complete, nationwide transition to paper ballot voting machines and the implementation of risk limiting audits ("RLAs"), an efficient and effective check on election results, to ensure security and confidence in electoral results. Encouragingly, many Illinois counties and multiple states have made significant progress in replacing their aging and DRE voting systems in recent months and years. Cook County, Macoupin County, Arkansas, Georgia, Pennsylvania and South Carolina have either completed

[21] *Federal Funds for Election Security: Will They Cover the Costs of Voter Marked*, Brennan Center for Justice and Verified Voting, 2018, https://www.brennancenter.org/our-work/research-reports/federal-funds-election-security-will-they-cover-costs-voter-marked-paper.

[22] California has required replacement by 2020, Wyoming is replacing now, and North Carolina state law currently requires replacement by December 31, 2019. "Secretary of State Alex Padilla Sets Deadline for Counties to Retire Old Voting Machines and Modernize Election Infrastructure," California Secretary of State Press Office, February 27, 2019, https://www.sos.ca.gov/administration/news-releases-and-advisories/2019/secretary-state-alex-padilla-sets-deadline-counties-retire-old-voting-machines-and-modernize-election-infrastructure; "Funding Elections Technology," National Conference of State Legislatures, July 29, 2019, http://www.ncsl.org/research/elections-and-campaigns/funding-election-technology.aspx; "State Board to Consider Certification of Voting Systems," *North Carolina State Board of Elections*, July 23, 2019, https://www.ncsbe.gov/Press-Releases?udt_2226_param_detail=767 ("Under current state law, DREs will be decertified in North Carolina on December 1, 2019, in favor of voting equipment that results in paper ballots for all voters. Proposed legislation pending in the N.C. General Assembly would delay the decertification date.").

[23] Norden and Cordova, "Voting Machine Security".

the replacement of their DRE voting machines or are transitioning now.[24] In addition, election officials in at least 6 additional states are piloting risk-limiting audits, the "gold-standard" of post-election audits.[25]

ii. Multiple Illinois Counties Use Electronic Pollbooks. There Are No Federal or State Security Guidelines for Electronic Pollbooks. They Should Be Included in the Federal Certification Process and Illinois Should Consider Adopting a State Certification Process and Common-Sense Contingency Policies.

As of July 2019, 41 states, including Illinois, and DC use or authorize the use of electronic pollbooks in at least some polling places.[26] Electronic pollbooks (EPBs) are laptops or tablets that poll workers use instead of paper lists to look up voters. Most EPBs can communicate with other EPBs in the same polling location to share real-time voter check-in updates.[27] In addition to an expedited check-in procedure, shorter lines, lower staffing needs, and cost savings, one major benefit of EPBs is that they can make it easier to set up "vote centers" during early voting in some states, e.g., Illinois, or on Election Day in other states. Vote centers are "an alternative to traditional neighborhood-based precincts"[28] Anyone in a particular jurisdiction can vote there, regardless of where they live, possibly making voting more convenient, providing additional cost savings, and encouraging increased voter turnout.[29] If a county uses multiple vote centers, the electronic pollbooks can automatically sync during the day to ensure that once someone has voted in a particular location, they cannot vote in another location on the same day.

Despite these advantages, EPBs also have the potential to introduce cybersecurity risks. In a worst-case scenario, hackers could alter or delete voter data, even causing voters to appear as if they have voted when they have not. EPBs that require access to the Internet can also pose

[24] Marley Arechiga, "Cook County Getting New Voting Machines For First Time In 13 Years," *WBEZ*, March 26, 2019, https://www.wbez.org/shows/wbez-news/cook-county-getting-new-voting-machines-for-first-time-in-13-years/02665912-4298-4ac5-afe8-3b7bff079027; Macoupin County Clerk's Office, "We are really excited that the County Board approved purchasing new voting machines at this week's meeting," Facebook, August 16 2019, https://www.facebook.com/MacoupinCountyClerk.

[25] Norden and Cordova, "Voting Machine Security".

[26] "Electronic Poll Books," National Conference of State Legislatures, July 15, 2019, http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx; Andrea Cordova, "Want a Simple Way to Increase Election Security? Use Paper," *Brennan Center for Justice*, October 8, 2018, https://www.brennancenter.org/blog/want-simple-way-increase-election-security-use-paper.

[27] Edgardo Cortés, Liz Howard, and Lawrence Norden, Better Safe than Sorry: How Election Officials can Plan Ahead to Protect the Vote in the Face of a Cyberattack, Brennan Center for Justice, 2018, https://www.brennancenter.org/sites/default/files/publications/2018_08_13_ElectionSecurity_V4.pdf.

[28] "Vote Centers," National Conference of State Legislatures, http://www.ncsl.org/research/elections-and-campaigns/vote-centers.aspx.

[29] Ibid.

problems in rural counties that lack reliable connectivity.[30] Unlike voting machines, there are currently no Illinois or national security standards for electronic pollbooks. Currently, the Help America Vote Act (HAVA), limits the federal election administration agency's ability to create requirements for, test, and certify EPBs in the same way they do for voting machines. The Illinois State Board of Elections is subject to similar limitations and expanding the state voting equipment certification process to include EPBs would likely require legislative action.

In the absence of federal certification standards, twelve states have developed a statewide system of e-pollbook regulation and certification according to the National Conference of State Legislatures (NCSL) and some states have adopted common sense contingency policies to ensure that voting can continue with minimal interruptions in the event of a successful EPB attack or failure.[31] In 2018, when 34 states used EPBs, only half required printed backup paper pollbooks to be present in the polling place at the time voting began and, in 32 of the 34 states, we found no requirements in state law or regulation mandating a minimum number of provisional ballots.[32] Although some Illinois counties, such as Cook County[33], voluntarily supply each polling place with a paper copy of the pollbook, or implement other common sense contingency policies, Illinois should consider adopting an EPB certification process and appropriate EPB contingency measures.

The Brennan Center supports updating HAVA to allow the Election Assistance Commission (EAC) to create a certification program for all electronic pollbooks, as they do for voting systems, in order to encourage secure EPB systems nationwide. These additional responsibilities will require increased funding and staffing levels for the EAC to effectively test and certify EPBs.

C. A comprehensive approach to election security requires Congressional leadership and partnership with federal, state and local election officials.

While state and local election officials can take many important steps without congressional action, these efforts will result in a patchwork of election infrastructure vulnerabilities across the country. Only Congress can establish minimum national election security standards to safeguard our election infrastructure and Americans' confidence in our electoral system. Congress should take several meaningful and simple steps to assist and support the ongoing efforts of state and local election officials to ensure that our elections are free, fair and secure.

[30] Andrea Cordova, "Want a Simple Way to Increase Election Security? Use Paper," *Brennan Center for Justice*, October 8, 2018, https://www.brennancenter.org/blog/want-simple-way-increase-election-security-use-paper.

[31] "Electronic Poll Books," National Conference of State Legislatures, July 15, 2019, http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx.

[32] Cordova, "Want a Simple Way to Increase Election Security? Use Paper".

[33] "Election Security," Cook County Clerk's Office, https://www.cookcountyclerk.com/service/election-security.

i. Congress should require election system vendors to report cybersecurity incidents.

Private companies are contracted to perform everything 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 poll books. Congress should consider additional steps to protect our elections from attacks that target these private election system vendors and to regulate vendor conduct. Unlike other sectors that the federal government has designated "critical infrastructure," there is currently almost no federal oversight of the private vendors who design, build and maintain our election systems. 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 elections infrastructure.

The Brennan Center recommends that Congress adopt a mandatory reporting system for all cyber security incidents for election vendors. While this may seem like a small step, it could have a large impact on the overall security position of election officials around the country. We know that the lack of transparency in vendor security is a significant vulnerability to election security. Private vendors were targeted in the 2016 election and are likely to be targeted again.[34] 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 similar critical infrastructure sectors.[35] The Brennan Center has documented some of the additional reasons for mandating such reporting in the 2010 report, *Voting System Failures: A Database Solution*.[36]

ii. Congress should make the critical infrastructure designation permanent.

[34] Lawrence Norden and Ian Vandewalker, *Securing Elections from Foreign Interference*, Brennan Center for Justice, 2017, https://www.brennancenter.org/publication/securing-elections-foreign-interference.

[35] Brian Calkin et al., *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.

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

In a decision subsequently affirmed by the Trump administration,[37] DHS Secretary Jeh Johnson designated election systems as "critical infrastructure" in January of 2017.[38] This designation is given to "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[39] It is significant because it "enables DHS to prioritize cybersecurity and physical security assistance to election officials upon request."[40] Further, this designation emphasizes, both domestically and internationally, that election infrastructure possesses all the benefits and protections that the Nation has to offer.[41] "Finally, a designation makes it easier for the federal government to have full and frank discussions with key stakeholders regarding sensitive vulnerability information."[42]

In practice, this designation has resulted in many substantive partnerships and collaborations. For example, it "enabled DHS to lead the formation of an Election Infrastructure Subsector Government Coordinating Council (EIS GCC) and the private sector's Election Infrastructure Subsector Sector Coordinating Council (EISCC) to serve as collaborative forums where the Federal Government, state and local government officials, and the private sector can establish mutually recognized information sharing to prevent or mitigate the effects of incidents that undermine the integrity of or public confidence in the election system."[43]
Congress should make this designation permanent to guarantee states are provided with priority access to tools and resources available from DHS and greater access to information on cyber vulnerabilities on a voluntary basis.

iii. Congress should provide consistent and reliable funding for election security.

[37] *Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure*, Office of Inspector General, Department of Homeland Security, February 28, 2019, https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-24-Feb19.pdf ("Subsequently, Secretary John Kelly affirmed the designation during a Congressional hearing on June 6, 2017"); Chase Gunter, "DHS secretary reaffirms support for voting systems' critical infrastructure designation," *GCN*, June 7, 2017, https://gcn.com/articles/2017/06/07/voting-systems-critical-infrastructure.aspx (" 'I don't believe we should' back off on the critical infrastructure designation, [DHS Secretary John Kelly] told members of the Senate Homeland Security and Governmental Affairs Committee on June 6").

[38] "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," Office of the Press Secretary, U.S. Department of Homeland Security, January 6, 2017, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

[39] "Statement by Secretary Jeh Johnson," DHS.

[40] *Election Infrastructure Security Resource Guide*, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, May 2019, https://www.dhs.gov/sites/default/files/publications/19_0531_cisa_election-security-resources-guide-may-2019.pdf.

[41] Ibid.

[42] "Statement by Secretary Jeh Johnson," DHS.

[43] *Election Infrastructure Security Resource Guide*, CISA.

A lack of financial resources presents the most significant obstacle to election security improvements in local jurisdictions. Congress took an important first step in 2018 by allocating $380 million to states for election security activities, and there are promising signs of more funding coming in 2019. But these one-time investments are not enough to address the significant problems facing election systems or provide long-term stability for future election security planning. It is clear there is an ongoing need for federal funding to help protect our election infrastructure from foreign threats. As such, we recommend that the federal government increase its funding commitment to election security and invest in innovative approaches toward making elections more secure, accessible, and efficient.

Because the threats to election security evolve over time, effective election security requires an ongoing commitment of resources, as opposed to a one-time expenditure. Companies in the private sector have departments and budgets dedicated to security generally, and often to cybersecurity specifically, precisely for this reason. Congress should provide a steady stream of funding for the periodic replacement of outdated voting systems, upgrading of databases and other election infrastructure, and the purchasing of ongoing technical and security support for all these systems.

The Brennan Center has estimated the nationwide five-year cost for four of the highest priority election security projects to be approximately $2.2 billion.[44] This total includes estimated costs for: 1) providing additional state and local election cybersecurity assistance, 2) upgrading or replacing statewide voter registration systems, 3) replacing aging and paperless voting machines, and 4) implementing rigorous post-election audits.

Conclusion

Election officials in Illinois and across our nation have made great progress since 2016 in securing our elections. But in an era when Americans' confidence in our democracy is at stake and 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." Doing so requires consistent, coordinated resources and leadership from all levels, including Congress, federal agencies, the states, and local governments.

[44] Lawrence Norden and Edgardo Cortés, "What Does Election Security Cost?," *Brennan Center for Justice*, August 15, 2019, https://www.brennancenter.org/our-work/analysis-opinion/what-does-election-security-cost.