Securing Our Elections

*Addressing Vulnerabilities Through Policy Recommendations*

Civic Analytics and Urban Intelligence, Fall 2020

**Background**

The purpose of this paper is to highlight several key vulnerabilities in the makeup of the current election infrastructure and propose recommendations for how to improve these processes to protect the security and integrity of elections.

**Areas of Recommendation**

* + Secure Voting Equipment
  + Regulate Election Vendors
  + Centralize Failures
  + Provide Continuing Support

**Secure Voting Equipment**

Replace Paperless Voting Machines

In a memo released by the Senate Select Committee on Intelligence Chairman, Senator Burr, the committee as a whole made a series of recommendations for improvements to election systems in conjunction with their investigations into the 2016 election interference events. Notably the committee encouraged states to “rapidly replace outdated and vulnerable voting systems” and insisted all machines have a “voter-verified paper trail” as a minimum requirement.[[1]](#footnote-1) The key vulnerability here is that paperless voting machines do not provide a physical backup of the votes recorded and therefore make performing recounts or post-election audits unreliable or impossible. Additionally many of the machines in use are nearing their estimated lifespan of 10-20 years. General trends would suggest that most states are moving in the right direction towards replacing antiquated equipment. In 2017, Michigan began replacing its machines with new optical-scan voting systems.[[2]](#footnote-2) Virginia decertified its use of paperless Direct Recording Electronic (DRE) voting machines after a hacking convention demonstrated how vulnerable to attacks several of the very models used in the state were.[[3]](#footnote-3) These practices have continued through the past few years with Arkansas, Delaware, and most recently, Georgia, South Carolina, and Pennsylvania opting to change to paper-based scanning systems.

**Regulate Election Vendors**

Much of the work done to improve the security of election systems in the United States has focused on how states and counties can better conduct themselves to ensure integrity of the election process. Little to no emphasis has been placed on providing more oversight to the private vendors who design and develop systems used at all stages of the election process, from registration database software, to electronic pollbooks and voting machines, to results reporting applications and post-election recount procedures.

Certification Process for Election System Vendors

The Election Assistance Commission (EAC) is the federal agency responsible for certifying voting machines used in elections. They do not, however, have a similar process for certifying vendors who produce this equipment or who provide other election services such as electronic pollbooks or results reporting applications. There is no oversight to ensure that these private vendors utilize best practices of security measures when developing their systems or for screening employees who program machines or conduct management and maintenance of equipment. As was seen with the issues around the Iowa Caucus App of this past year, lack of oversight can result in poorly developed solutions and critical malfunctions when the services are tested at scale. These hiccups only sow more distrust into the election process and instill an uneasiness in voters regarding the integrity of how elections are conducted. The certification process used by the EAC should be expanded to cover all stages of the election process and provide increased accountability into how private vendors develop and deploy their services.

**Centralize Failures**

Information sharing is a critical element to better understanding why failures happen in voting machine systems and what can be done to reduce their occurrences in the future. As the federal agency responsible for overseeing election infrastructure, the EAC should take more substantive role in organizing this information and managing its distribution among states.

National Database of Voting System Failures

Currently there is no unified resource for election officials to access information about past voting system failures. This means that the same issues occur from the same machines, in the same states or different states, and across different elections over time. Many of these occurrences were likely preventable given proper record keeping and information sharing. A publicly accessible database should be created where both election officials and voters who experience machine issues can submit records of the failures. This resource would be managed and maintained by the EAC. An extensive report conducted by the Brennan Center and published over a decade ago outlines the idea for a database solution and details many case studies of system failures.[[4]](#footnote-4) To build upon their foundation, the mandate of the EAC should be expanded to allow the agency to operate as an investigative body into the claims collected in the database. The agency should operate similarly to how the National Transportation Safety Board does, serving as the body of experts to investigate, subpoena, and question representatives from the companies who produce these machines to explain the incidents of failure and how the vendors propose to reform their systems to decrease the likelihood of these incidents. There must be enforcement and consequence behind not complying or there is little incentive for private actors to cooperate. The EAC should be allowed to levy fines against private companies who do not comply and should move aggressively to decertify systems and vendors who refuse to address vulnerabilities in their systems.

**Provide Continuing Support**

Improvement of election system infrastructure should not be considered a one-time investment. The solutions laid out in this report will require continued attention and adaptation as the technology used in elections continues to evolve.

“Critical Infrastructure” Designation

In January of 2017 the Department of Homeland Security designated election infrastructure as “critical infrastructure” under the Government Facilities sector. Through the Cybersecurity and Infrastructure Security Agency (CISA) this designation allows access to a variety of services for state and local election officials to reduce both cyber and physical risk to their election systems. These services include, communication with cybersecurity advisors, risk and vulnerability assessments in physical and cyber spaces, information sharing through National Awareness System alerts, and training for self-sufficient maintenance of systems.[[5]](#footnote-5) This special designation may be rescinded by the executive at any time but that would be a mistake. To protect access to these additional services, Congress should permanently enforce the recognition of election infrastructure as critical through passage of legislation.

Sufficiently Fund the Election Assistance Commission

Funding for the EAC has remained stagnant or declined over the past decade and only received an increase in 2020 because of the Covid-19 crisis and the expansive escalation of vote-by-mail programs across many states. Figure 3 in the appendix shows a graph of the agency’s budget for the past decade. In order to successfully meet its broadened responsibilities as an investigative agency, the EAC should be properly funded in all future federal budgets. Estimates on figures for cost of adequately funding the agency and election services can be found in a Brennan Center report on election security costs.[[6]](#footnote-6)

**Conclusion**

Since the events of the 2016 Presidential election were uncovered, the United States has made significant efforts to improve the physical and cyber elements of its election systems in a effort to improve the security of its elections and reduce general concern over election interference from domestic and foreign actors. Many of these steps have shown positive results and are supported by the recent statement by CISA characterizing the 2020 Presidential election as “the most secure in American history.”[[7]](#footnote-7) The general trends by states are encouraging, as most move to replace outdated and paperless voting machines with more secure alternatives that require paper records, ensuring physical copies of votes exist and are present to be used in post-election audits and recounts. There are still many areas for improvement however, notably in the role the federal government and agencies like the Election Assistance Commission take as oversight bodies to all elections. The recommendations laid out in this paper would be significant steps to carry forward the direction of securing our elections fully.

**Appendix**

Figure 1 — Direct Recording Electronic Machine Use by State

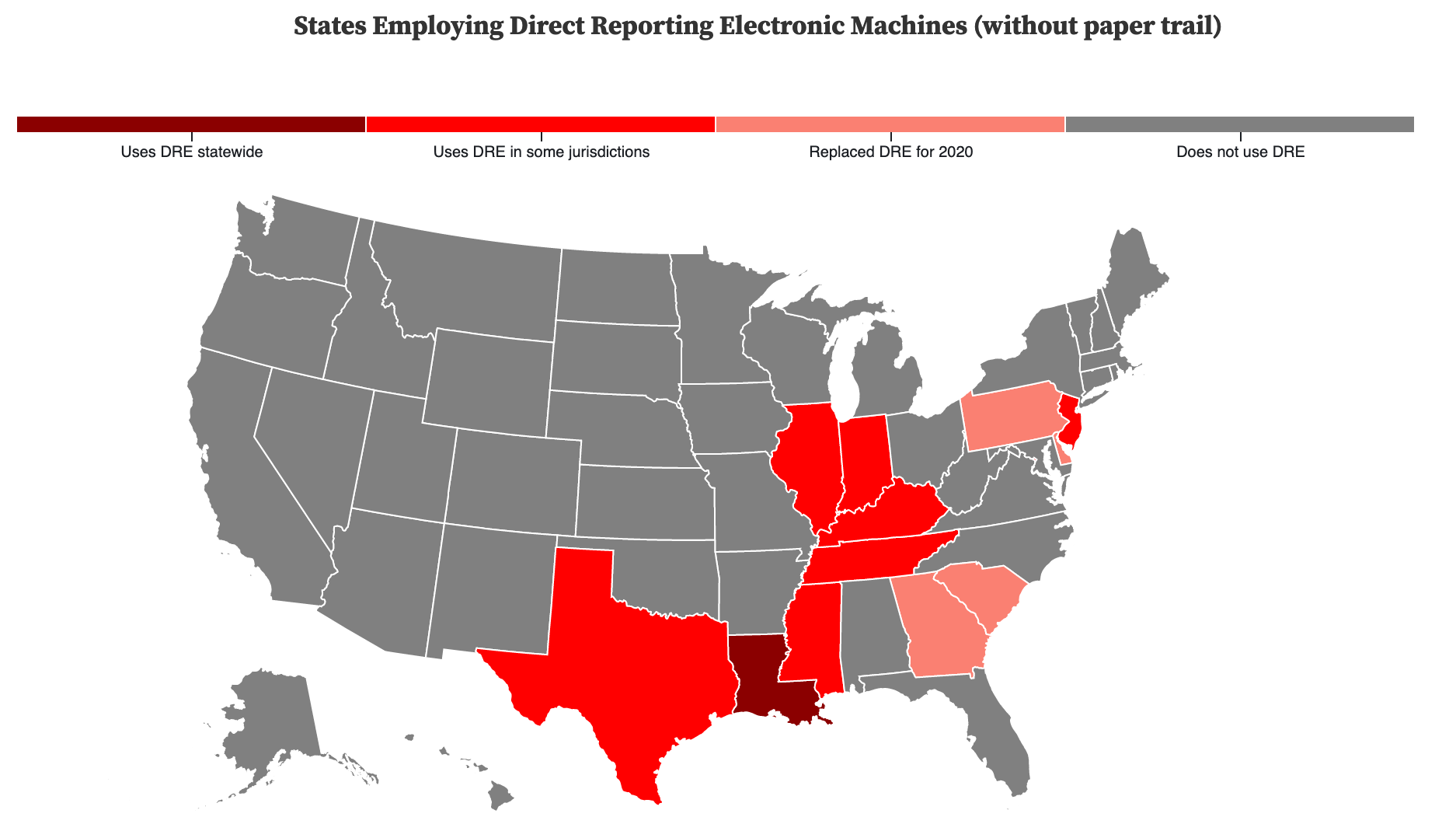
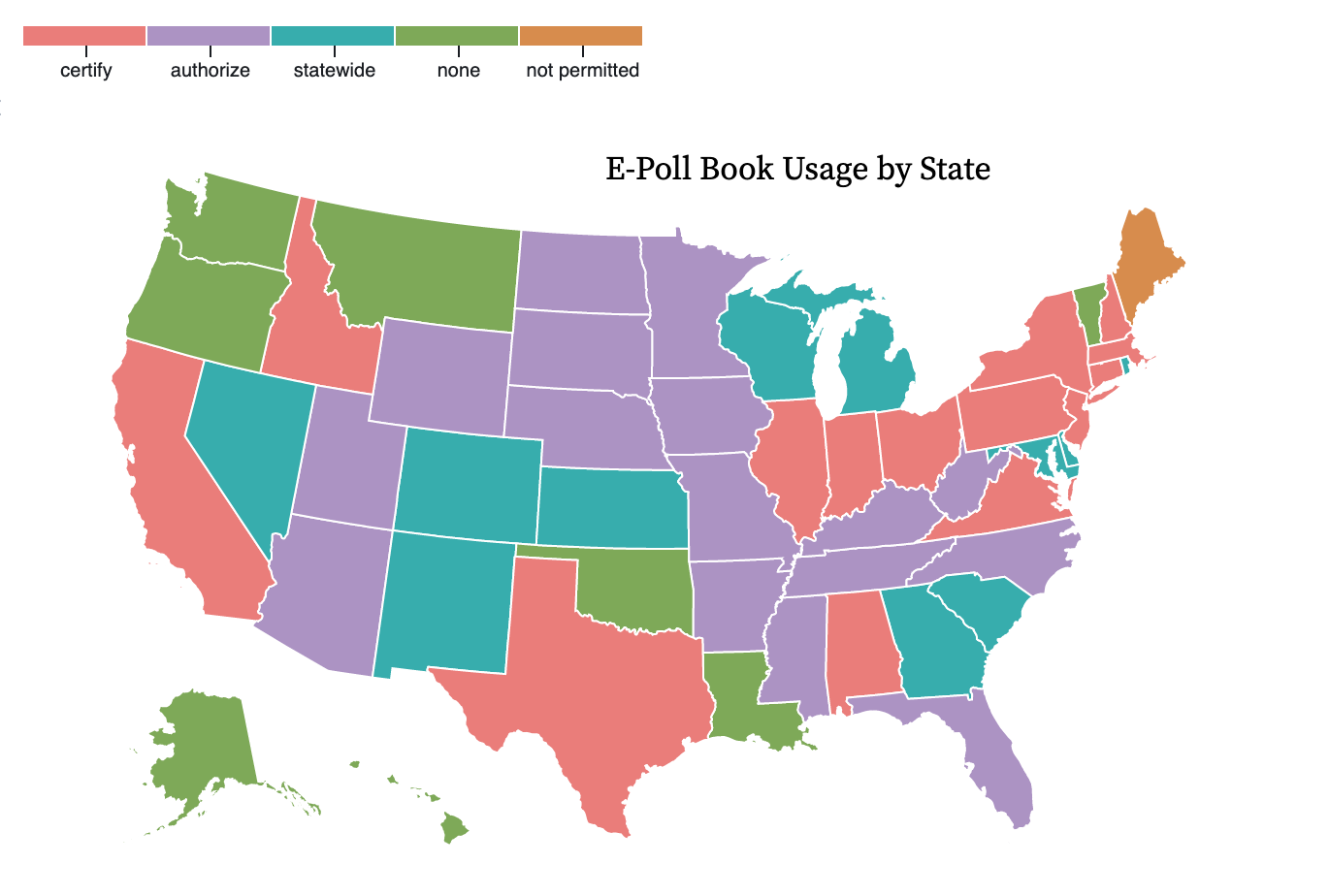
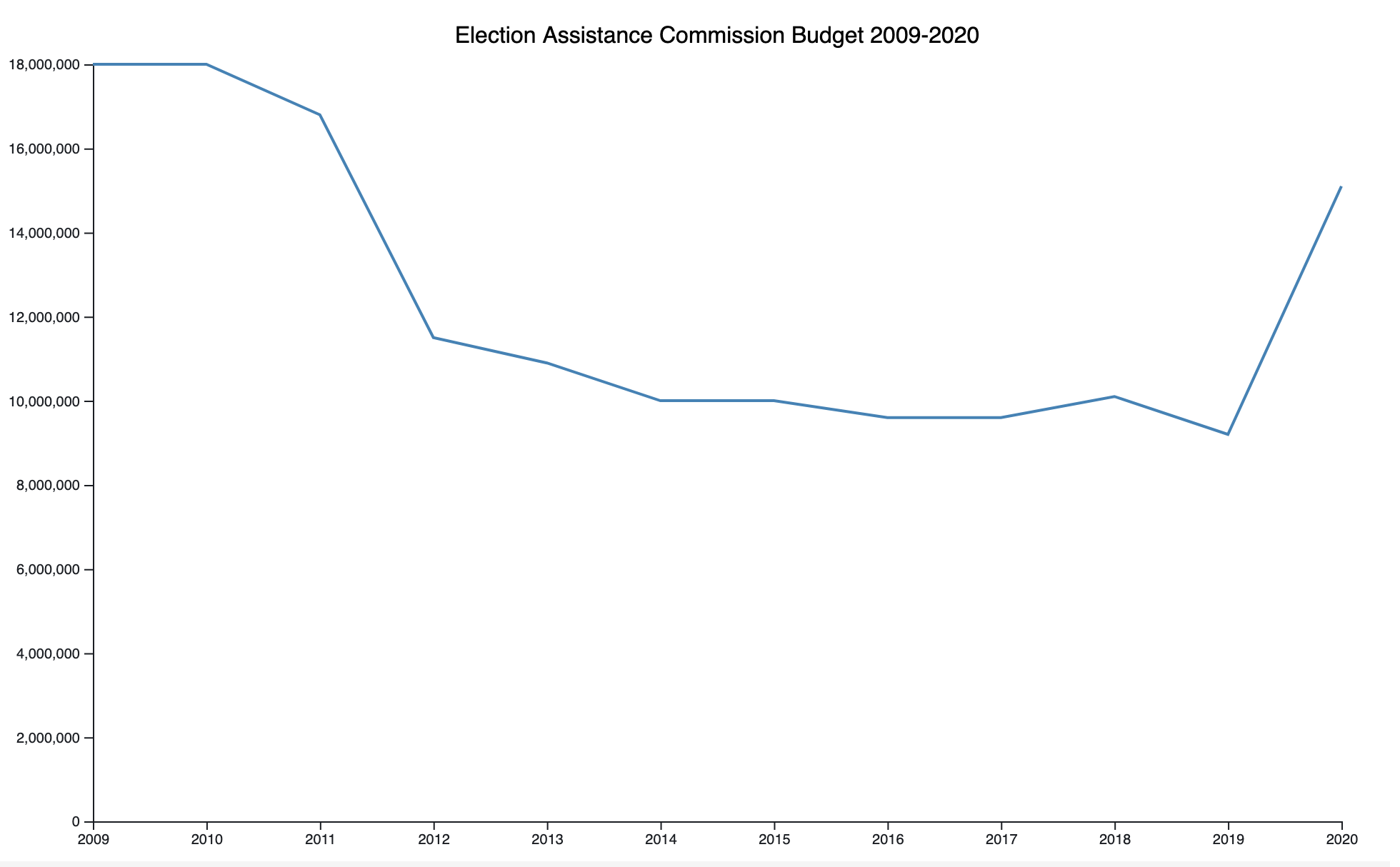
This map shows the use of paperless Direct Recording Electronic machines by state. The majority of states (grey) do not use any paperless DRE machines in their elections. The map reflects recent changes by several states (Delaware, Pennsylvania, South Carolina, and Georgia) to replace their DRE machines with more secure alternatives, namely optical scanners. The raw data used to produce this map was collected from the *Election Administration and Voting Survey 2018 Report* produced by the Election Assistance Commission.[[8]](#footnote-8)

Figure 2 — Electronic Poll Book Use by State

This map shows the distribution and classification of electronic poll book (e-pollbook) use by state. The use of electronic poll books in elections has been on the rise since 2016, with an increase of nearly 48% between 2016 and 2018.[[9]](#footnote-9) Electronic poll books are typically custom designed software installed on tablets and have the capability of providing a variety of functions beyond recording the attendance of a voter at a polling site. Because many are generated in conjunction with registration databases, e-pollbooks can assist with: redirecting voters in the wrong location to correct polling places, scanning licenses or other government IDs to retrieve voter’s information, search registration records beyond the scope of precinct or county, allow for real-time updating of voter registration record or voter history, notify poll workers of voters who may have voted absentee or during an early voting period, and register voters under same-day registration procedures. Currently there are 13 states (red) who have created certification programs for allowing the use of electronic pollbooks in their elections. 12 states (blue) provide statewide procedures for e-pollbook use but have no formal certification process. 15 states (purple) authorize the use of e-pollbooks but do not have certification or statewide policies, typically leaving usage at the discretion of the Secretary of State and county level election officials. The information for this map was obtained from the 2018 EAC report and from the National Conference of State Legislatures.[[10]](#footnote-10) The implementation of a national certification program for electronic pollbooks is another area of consideration for recommendation when looking to expand the responsibilities of the Election Assistance Commission.

Figure 3 — Election Assistance Commission Budget, 2009-2020

This graph shows the change in the budget of the Election Assistance Commission over the years of 2009 to 2020. The general trend is that the budget has declined or remained stagnant over the decade+ and only saw significant increase in the last year because of the impact of Covid-19 on carrying out traditional election processes. In 2019 the budget was just over $9 million dollars, roughly half of what it was at the start of the decade. The EAC budget should be restored to its former height if not increased further to adequately cover the necessary staff to perform its established role as the certifying entity of election system infrastructure and its new role as an investigative body into failures and malfunctions. The information for this graph was collected from budget reports on the Election Assistance Commission website.[[11]](#footnote-11)

**Interviews Conducted**

* + *Oscar Romero* — Program Director, Innovation, Mayor’s Office of the Chief Technology Officer, New York City
  + *Shanna Crumley* — Innovation Advisor, Mayor’s Office of the Chief Technology Officer, New York City
  + *Aileen Kim* — Communications Representative, Tusk Philanthropies and Mobile Voting Project
  + *Daniel Abramson* — Communications Director, Civic Engagement Commission, New York City
  + *Okwudiri Onyedum* — Member, Voter Assistance Advisory Committee, New York City Campaign Finance Board

1. <https://www.burr.senate.gov/imo/media/doc/One-Pager%20Recs%20FINAL%20VERSION%203-20.pdf> [↑](#footnote-ref-1)
2. https://www.freep.com/story/news/2017/08/02/voting-machines-primary-election-michigan/532782001/ [↑](#footnote-ref-2)
3. https://www.washingtonpost.com/local/virginia-politics/virginia-scraps-touch-screen-voting-machines-as-election-for-governor-looms/2017/09/08/e266ead6-94fe-11e7-89fa-bb822a46da5b\_story.html?utm\_term=.aef3881243f2 [↑](#footnote-ref-3)
4. https://www.brennancenter.org/sites/default/files/2019-08/Report\_Voting\_Machine\_Failures\_Database-Solution.pdf [↑](#footnote-ref-4)
5. https://www.dhs.gov/topic/election-security [↑](#footnote-ref-5)
6. https://www.brennancenter.org/our-work/analysis-opinion/what-does-election-security-cost [↑](#footnote-ref-6)
7. https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election [↑](#footnote-ref-7)
8. https://www.eac.gov/sites/default/files/eac\_assets/1/6/2018\_EAVS\_Report.pdf [↑](#footnote-ref-8)
9. https://www.eac.gov/sites/default/files/eac\_assets/1/6/2018\_EAVS\_Report.pdf [↑](#footnote-ref-9)
10. https://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx [↑](#footnote-ref-10)
11. https://www.eac.gov/about-eac/budget-and-finance [↑](#footnote-ref-11)