2020 ELECTION SECURITY—PERSPECTIVES FROM VOTING SYSTEM VENDORS AND EXPERTS

HEARING

BEFORE THE

COMMITTEE ON HOUSE ADMINISTRATION
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

JANUARY 9, 2020

Printed for the use of the Committee on House Administration

Available on the Internet:
http://www.govinfo.gov/committee/house-administration

2020 ELECTION SECURITY—PERSPECTIVES FROM VOTING SYSTEM VENDORS AND EXPERTS

2020 ELECTION SECURITY—PERSPECTIVES FROM VOTING SYSTEM VENDORS AND EXPERTS

HEARING

BEFORE THE

COMMITTEE ON HOUSE ADMINISTRATION HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

JANUARY 9, 2020

Printed for the use of the Committee on House Administration

Available on the Internet:
http://www.govinfo.gov/committee/house-administration

U.S. GOVERNMENT PUBLISHING OFFICE
41–318 WASHINGTON : 2020

Committee on House Administration

ZOE LOFGREN, California, *Chairperson*

JAMIE RASKIN, Maryland
SUSAN A. DAVIS, California
G. K. BUTTERFIELD, North Carolina
MARCIA L. FUDGE, Ohio
PETE AGUILAR, California

RODNEY DAVIS, Illinois,
Ranking Member
MARK WALKER, North Carolina
BARRY LOUDERMILK, Georgia

CONTENTS

JANUARY 9, 2020

OPENING STATEMENTS

WITNESSES

QUESTIONS FOR THE RECORD

SUBMISSIONS FOR THE RECORD

[1] Mr. Blaze did not answer submitted questions for the record by the time of printing.

2020 ELECTION SECURITY—PERSPECTIVES FROM VOTING SYSTEM VENDORS AND EXPERTS

THURSDAY, JANUARY 9, 2020

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOUSE ADMINISTRATION,
Washington, DC.

The Committee met, pursuant to call, at 10:03 a.m., in Room 1310, Longworth House Office Building, Hon. Zoe Lofgren [Chairperson of the Committee] presiding.

Present: Representatives Lofgren, Raskin, Davis of California, Butterfield, Fudge, Aguilar, Davis of Illinois, and Walker.

Staff Present: Sean Jones, Legislative Clerk; Jamie Fleet, Staff Director; Mariam Malik, Staff Assistant; Hannah Carr; Staff Assistant; Stephen Spaulding, Elections Counsel; Georgina Cannan, Elections Counsel; Peter Whippy, Communications Director; Eddie Flaherty, Chief Clerk; David Tucker, Senior Counsel and Parliamentarian; Courtney Parella, Minority Communications Director; Jen Daulby, Minority Staff Director; Cole Felder, Minority General Counsel; Tim Monahan, Minority Deputy Staff Director; and Nick Crocker, Minority Director, Member Services.

The CHAIRPERSON. Welcome, everybody, and good morning. We are waiting for Committee Members to arrive any moment, but while we are waiting we will begin with our opening statements.

I would like to note that our Committee is charged with overseeing the administration of Federal elections. Today's hearing will help us fulfill that responsibility by providing an opportunity to hear from the vendors of most of our country's voting systems. This is the first time the Chief Executive Officers of the three major vendors have appeared together in a congressional hearing. The companies they represent provide at least 80 percent of the estimated 350,000 voting machines in use today, reaching over 100 million registered voters.

However, despite their outsized role in the mechanics of our democracy, some have accused these companies of obfuscating and, in some cases, misleading election administrators and the American public. Others suggest there is an insufficient regulatory structure for this sector.

In the Committee's May 2019 hearing on election security, Lawrence Norden of the Brennan Center for Justice wrote in his testimony that, and I quote, "there are more Federal regulations for ballpoint pens and magic markers than there are for voting systems and other parts of our election infrastructure." There may be more work to do and much for Congress to learn about this industry.

Many have concerns about voting systems with remote access software, and I think we want to make sure that companies no longer sell voting machines that have network capabilities. In 2019, according to a report in Motherboard, a group of election security experts, they uncovered that backend election systems in at least 10 states were connected to the internet despite one company's claim that its systems were not.

We need also to understand supply chains. In December 2019, a study released by Enteros, a supply chain monitoring company, showed that one-fifth, or 20 percent, of the components in a popular voting machine came from China-based companies. Furthermore, close to two-thirds or actually 59 percent of suppliers within that machine's supply chain had locations in either China or Russia. Enteros didn't name the vendor that manufactured the voting machine but said that it was widely used.

I have also heard concerns about the ownership and control of voting machine vendors. Public reporting indicates that all three of the major voting system vendors represented here today are privately held or are partially controlled by private equity firms. I believe it is in the public interest for Congress to better understand who could financially benefit from the administration of our elections.

There are also, of course, threats to our voting infrastructure. We learned in Special Counsel Mueller's report that Russia intelligence officers targeted employees of a voting technology company that developed software to manage voter rolls and installed malware on the company network. We also know that our own voluntary voting system guidelines have not been substantially updated since 2005 before the iPhone was even available. It then took the EAC another decade to make small changes, which were adopted in 2015, almost 5 years ago.

So there is more we have to do together to bolster public confidence and trust in our election systems. That is why this Congress has acted. Last June, the House passed H.R. 2722, the SAFE Act, that would require individual durable voter verified paper ballots. It would require strict cyber security standards. It would require risk-limiting audits, prohibit wireless and internet connectivity, and create accountability mechanisms for election technology vendors. The bill awaits consideration in the Senate.

Just last month, Congress appropriated $425 million to the States to improve election security. This builds on the $380 million Congress appropriated in 2018. Securing our elections should not be a partisan issue. Election security is about upholding a democracy of, by, and for the people, the American people, be they Republican, Democratic, third party, or no party at all. Our democracy is resilient, but it relies on everyone having their vote counted as cast.

I now recognize our Ranking Member, Mr. Davis, for any opening statement he may wish to make.

[The statement of The Chairperson follows:]

ZOE LOFGREN, CALIFORNIA
CHAIRPERSON

JAMIE RASKIN, MARYLAND
VICE CHAIRPERSON

SUSAN DAVIS, CALIFORNIA
G.K. BUTTERFIELD, NORTH CAROLINA
MARCIA FUDGE, OHIO
PETE AGUILAR, CALIFORNIA

JAMIE FLEET, STAFF DIRECTOR

Congress of the United States
House of Representatives
COMMITTEE ON HOUSE ADMINISTRATION
1309 Longworth House Office Building
Washington, D.C. 20515–6157
(202) 225–2061
https://cha.house.gov

RODNEY DAVIS, ILLINOIS
RANKING MINORITY MEMBER

MARK WALKER, NORTH CAROLINA
BARRY LOUDERMILK, GEORGIA

ONE HUNDRED SIXTEENTH CONGRESS

JEN DAULBY, MINORITY STAFF DIRECTOR

Chairperson Zoe Lofgren
2020 Election Security – Perspectives from Voting System Vendors and Experts
January 9, 2020
Opening Statement

This Committee is charged with overseeing the administration of Federal elections. Today's hearing will help us fulfill this responsibility by providing an opportunity to hear from the vendors of most of our country's voting systems. This is the first time the CEOs of the three major vendors have appeared together in a congressional hearing. The companies they represent provide at least 80 percent of the estimated 350,000 voting machines in use today, reaching over 100 million registered voters.

However, despite their outsized role in the mechanics of our democracy, some have accused these companies of obfuscating and, in some cases, misleading election administrators and the American public. Others suggest there is an insufficient regulatory structure for this sector.

During the Committee's May 2019 hearing on election security, Lawrence Norden of the Brennan Center for Justice wrote in his testimony that, and I quote, there are more Federal regulations for ballpoint pens and magic markers than there are for voting systems and other parts of our election infrastructure. There is much work to do and much for Congress to learn about this industry.

Many have concerns about voting systems with remote access software. We want to make sure that companies no longer sell voting machines that have network capabilities. In 2019, according to a report in Motherboard, a group of election security experts, they uncovered that backend election systems in at least 10 states were connected to the internet despite one company's claim that its systems were not.

We need also to understand supply chains. In December 2019, a study released by Enteros, a supply chain monitoring company, showed that one fifth, or 20 percent, of the components in a popular voting machine came from China based companies. Furthermore, close to two thirds or actually 59 percent of suppliers within that machine's supply chain had locations in either China or Russia. Enteros did not name the vendor that manufactured the voting machine but said that it was widely used.

I have also heard concerns about the ownership and control of voting machine vendors. Public reporting indicates that all three of the major voting system vendors represented here today are privately held or are partially controlled by private equity firms. I believe it is in the public interest for Congress to better understand who could financially benefit from the administration of our elections.

There are also threats to our voting infrastructure. We learned in Special Counsel Mueller's report that Russia intelligence officers targeted employees of a voting technology company that developed software to manage voter rolls and installed malware on the company network. We also know that our own voluntary voting system guidelines have not been substantially updated since 2005 before the iPhone was even available. It then took the EAC another decade to make small changes, which were adopted in 2015, almost five years ago.

There is more we must do together to bolster public confidence and trust in our election systems. That is why this Congress has acted. Last June, the House passed H.R. 2722, the SAFE Act, that would require individual durable voter verified paper ballots. It would require strict cyber security standards. It would require risk limiting audits, prohibit wireless and internet connectivity, and create accountability mechanisms for election technology vendors. The bill awaits consideration in the Senate.

Just last month, Congress appropriated $425 million to the States to improve election security. This builds on the $380 million Congress appropriated in 2018. Securing our elections should not be a partisan issue. Election security is about upholding a democracy of, by, and for the people, the American people, be they Republican, Democratic, third party, or no party at all.

Our democracy is resilient, but it relies on everyone having their vote counted as cast.

I now recognize our ranking member, Mr. Davis, for any opening statement he may wish to make.

Mr. DAVIS of Illinois. Thank you, Madam Chairperson. Especially, also thank you for holding this necessary, long overdue hearing that I've been looking forward to since the beginning of this Congress. I also want to thank all of our witnesses for taking the time to be here today to discuss the very important issues regarding elections and election security and elections administration.

My agenda since becoming the Ranking Member of this Committee has been and continues to be focused on nonpartisan and effective oversight of our Nation's elections, which are maintained by the States, not the Federal Government. But that does not mean that this Committee and the House itself does not have an important oversight role to play in securing elections.

Our witnesses here today have state, county, and local jurisdictions as clients who know their electorate best. We also have witnesses who have experience with running those elections, but we know that threats from foreign actors to our Nation's elections are not going away.

It should be noted from the Senate Intelligence Committee's report on the 2016 election, there were, quote, "no indications that votes were changed, vote tallying systems were manipulated, or that any voter registration data was altered or deleted,", by Russia or any foreign actor.

DHS Assistant Secretary Jeanette Manfra said in the Senate Intel's opening hearing in June of 2017 that, quote, "we do not—we do have confidence in the overall integrity of our electoral system because our voting infrastructure is fundamentally resilient.". While we have faith in the electoral system, we still have a responsibility to strengthen the relationship between States and the Federal Government to ensure that Americans' votes are and will continue to be protected.

There has been some disagreement with my colleagues across the aisle on how best to accomplish this mission, but I believe our goal is the same. Instead of getting into a long-winded debate today between paper versus electronic, State versus Federal, let's instead focus our efforts on areas within our Federal reach that need improvement, areas where we may come to a bipartisan agreement as we have seen in this Committee and many times in the past.

This Committee created and passed the Help America Vote Act of 2002 (HAVA), which provided much-needed funds to states so that they could update their election security and voting infrastructure and created the Election Assistance Commission or EAC. One notable requirement of HAVA was for the EAC to create a set of specifications and requirements against which voting systems can be tested called the Voluntary Voting Systems Guideline, or VVSG. The EAC adopted the first VVSG in December of 2005 and approved an updated version, VVSG 1.1, in January of 2016. Now we are currently waiting for the EAC to produce the newest guidelines, the VVSG 2.0.

This year, our Committee should hold a hearing with the EAC to discuss this voting guideline development process and several other processes within our jurisdiction.

Perhaps we should not only focus on the EAC but, instead, HAVA itself. The Help America Vote Act was originally created in 2002 following the 2000 Presidential election and its many issues with paper ballots and ballot marking devices, much like we will be discussing today.

There have been many developments in voting systems technology that are not addressed in the original HAVA language like e-pollbooks and securing online registration databases. It has been almost 20 years since this law has been updated, and with the recent developments in election security and technology, it is time to modernize these laws again and incentivize new, more secure infrastructure development from vendors like each of you.

Also, let's recognize the steps we have taken this Congress alone to secure our elections. As Chairperson Lofgren said, the Fiscal Year 2020 National Defense Authorization recently enacted last month contained several provisions related to election security. Most involved providing Congress, Federal, or State agencies with information about election interference, something that was in the election security bill I introduced, H.R. 3412, the Election Security Assistance Act. It also requires the Director of National Intelligence, in coordination with several other agencies, to develop a strategy for countering Russian cyberattacks against U.S. elections, another provision I had in my bill.

In addition to the NDAA, the recent appropriations, as Chairperson Lofgren said, included $425 million for payments to States, territories, and the District of Columbia to make general improvements to the administration of Federal elections including upgrades to election technology and security.

Much has been done, but we still have much to do, which is why you are all here with us today. A fundamental right of our Nation's ability is to choose our leaders. The American people deserve that right to be protected. We should secure and protect our Nation's elections without partisan politics, and I hope we can remember that not only during this hearing but also for the duration of this Congress.

Thank you, Madam Chairperson. I yield back.

[The statement of Mr. Davis of Illinois follows:]

ZOE LOFGREN, CALIFORNIA
Chairperson

JAMIE RASKIN, MARYLAND
Vice Chairperson

SUSAN DAVIS, CALIFORNIA
G.K. BUTTERFIELD, NORTH CAROLINA
MARCIA FUDGE, OHIO
PETE AGUILAR, CALIFORNIA

Jamie Fleet, Staff Director

Congress of the United States
House of Representatives
COMMITTEE ON HOUSE ADMINISTRATION
1309 Longworth House Office Building
Washington, D.C. 20515–6157
(202) 225–2061
https://cha.house.gov

RODNEY DAVIS, ILLINOIS
Ranking Minority Member

MARK WALKER, NORTH CAROLINA
BARRY LOUDERMILK, GEORGIA

ONE HUNDRED SIXTEENTH CONGRESS

Jen Daulby, Minority Staff Director

Ranking Member Rodney Davis
2020 Election Security – Perspectives from Voting System Vendors and Experts
January 9, 2020
Opening Statement

Thank you, Madam Chairperson, and thank you for holding this necessary, long overdue hearing that I've been looking forward to since the beginning of this Congress. And thank you to our witnesses for taking the time to be here today to discuss the very important issues regarding elections and election security and elections administration.

My agenda since becoming the Ranking Member of this Committee has been and continues to be focused on nonpartisan and effective oversight of our Nation's elections, which are maintained by the States, not the Federal Government. But that does not mean that this Committee and the House itself does not have an important oversight role to play in securing elections.

Our witnesses here today have State, county, and local jurisdictions as clients who know their electorate best. We also have witnesses who have experience with running those elections, but we know that threats from foreign actors to our Nation's elections are not going away.

It should be noted from the Senate Intelligence Committee's report on the 2016 election, there were "no indications that votes were changed, vote tallying systems were manipulated, or that any voter registration data was altered or deleted" by Russia or any foreign actor.

DHS Assistant Secretary Jeanette Manfra said in the Senate Intel's opening hearing in June of 2017 that "we do have confidence in the overall integrity of our electoral system because our voting infrastructure is fundamentally resilient." While we have faith in the electoral system, we still have a responsibility to strengthen the relationship between States and the Federal Government to ensure that Americans' votes are and will continue to be protected.

There has been some disagreement with my colleagues across the aisle on how best to accomplish this mission, but I believe our goal is the same. Instead of getting into a winded debate today between paper versus electronic, State versus Federal, let's instead focus our efforts on areas within our Federal reach that need improvement, areas where we may come to a bipartisan agreement as we have seen in this Committee and many times in the past.

This Committee created and passed the Help America Vote Act of 2002, which provided much needed funds to States so that they could update their election security and voting infrastructure and created the Election Assistance Commission or EAC. One notable requirement of HAVA was for the EAC to create a set of specifications and requirements against which voting systems can be tested called the Voluntary Voting Systems Guideline, or VVSG. The EAC adopted the first VVSG in December of 2005 and approved an updated version, VVSG 1.1, in January of 2016. Now we are currently waiting for the EAC to produce the newest guidelines, the VVSG 2.0.

This year, our Committee should hold a hearing with the EAC to discuss this voting guideline development process and several other processes within our jurisdiction.

Perhaps we should not only focus on the EAC but, instead, HAVA itself. The Help America Vote Act was originally created in 2002 following the 2000 Presidential election and its many issues with paper ballots and ballot marking devices, much like we will be discussing today.

There have been many developments in voting systems technology that are not addressed in the original HAVA language like e pollbooks and securing online registration databases. It has been almost 20 years since this law has been updated, and with the recent developments in election security and technology, it is time to modernize these laws again and incentivize new, more secure infrastructure development from vendors like each of you.

Also, let's recognize the steps we have taken this Congress alone to secure our elections. As Chairperson Lofgren said, the Fiscal Year 2020 National Defense Authorization recently enacted last month contained several provisions related to election security. Most involved providing Congress, Federal, or State agencies with information about election interference, something that was in the election security bill I introduced, H.R. 3412, the Election Security Assistance Act. It also requires the Director of National Intelligence, in coordination with several other agencies, to develop a strategy for countering Russian cyber attacks against U.S. elections, another provision I had in my bill.

In addition to the NDAA, the recent appropriations, as Chairperson Lofgren said, included $425 million for payments to States, territories, and the District of Columbia to make general improvements to the administration of Federal elections including upgrades to election technology and security.

Much has been done, but we still have much to do, which is why you are all here with us today. A fundamental right of our Nation's ability is to choose our leaders. The American people deserve that right to be protected. We should secure and protect our Nation's elections without partisan politics, and I hope we can remember that not only during this hearing but also for the duration of this Congress.

Thank you, Madam Chair. I yield back.

The CHAIRPERSON. Thank you.

The gentleman yields back.

All other Members are invited to submit an opening statement for the record without objection.

At this point, I would like to welcome our witnesses. Thank you for being here today. Joining us are the President and CEO of Election Systems & Software, Mr. Tom Burt; President and CEO of Dominion Voting Systems, Mr. John Poulos; and President and CEO of Hart InterCivic, Julie Mathis.

I would like to introduce each of the witnesses. First, Mr. Burt. Tom Burt became President and CEO of Elections Systems & Software in 2015. He joined E&S in 2008, leading sales, customer services, operations, and the product departments. Before joining ES&S, Mr. Burt developed his general management and sales leadership at McMaster Carr, a supply company, and Anderson Consulting where he served in a variety of executive management roles.

John Poulos is the founding President and CEO of Dominion. In this role, he leads the company's overall business strategy and operations. Since its inception in 2003, Dominion has grown to support over 1,200 jurisdictions across North America. He holds a Bachelor of Arts degree in electrical engineering from the University of Toronto as well as a Master's of Business Administration degree from INSEAD, Fontainebleau, France.

Julie Mathis joined Hart in 2014 but became its CEO just 9 days ago, so congratulations. She has previously served as President and CFO of the company. Prior to joining Hart, she served as Vice President of finance at Dell. Ms. Mathis holds a Bachelor of Business Administration degree in accounting from the University of Texas at Austin and is a Certified Public Accountant.

I would at this point ask unanimous consent that all Members have 5 legislative days to revise and extend their remarks and their written statements be made part of the record.

And, without objection, that is so ordered.

I would also like to remind witnesses that their entire written statements will be made part of the record and that the record will remain open for at least five days for additional materials to be submitted.

At this point, I would ask each of the witnesses to stand and raise their right hand.

[Witnesses sworn.]

The CHAIRPERSON. The record will reflect that all three witnesses answered in the affirmative.

We will first recognize you, Mr. Burt, for your testimony.

TESTIMONY OF TOM BURT, PRESIDENT AND CEO, ELECTION SYSTEMS & SOFTWARE, OMAHA, NEBRASKA; JOHN POULOS, PRESIDENT AND CEO, DOMINION VOTING SYSTEMS, DENVER, COLORADO; AND JULIE MATHIS, PRESIDENT AND CEO, HART INTERCIVIC, AUSTIN, TEXAS.

TESTIMONY OF TOM BURT

Mr. BURT. Thank you.

Chairperson Lofgren, Ranking Member Davis, and Members of the House Administration Committee, thank you for the opportunity to testify on the vitally important subject of election security. My name is Tom Burt, and I am CEO of Elections Systems & Software. I'm encouraged to see the growing attention to stronger security for elections, and I'm thankful for the additional recent funding to the States provided by Congress under your leadership.

Founded 40 years ago, ES&S' headquarters are in Omaha, Nebraska, where roughly half of our 490 employees live and work. Others live locally in or near the States where we provide products and services, including employees who reside in California, Georgia, Illinois, Maryland, North Carolina, and Ohio.

Let me be clear and unequivocal with you: ES&S is committed to doing everything we can to safeguard our Nation's election security. It is what every one of our employees wakes up and goes to bed thinking about. For us, every single day is election day.

Additionally, I want to make clear that ES&S strongly supports Federal mandates for the following three policies: first, an auditable paper record for every vote cast; second, post-election audits of these paper records; and, third, more rigorous standards for the programmatic security testing of voting equipment by a federally controlled regulatory body.

I'd like to elaborate on a few of the many examples ES&S has raised—ways that ES&S has raised the bar on itself for election security and called on Congress to raise the bar on the entire industry. First, as mentioned, it is important that an auditable paper trail be required for every vote cast. ES&S has stopped selling new voting machines that do not produce an auditable paper record at the primary voting device.

Second, we support and applaud the increase in dedicated resources coming from Congress, State, and local officials, the Election Assistance Commission, and the Department of Homeland Security. We embrace our partnerships with these bodies because we believe that collectively we can provide necessary and continuous improvement in election security.

While the recent appropriations bill included additional elections-related funding from Congress, we believe the Federal Government needs to devote these resources to State and local jurisdictions on an annual basis.

Third, I'd like to highlight just a few of the many important steps ES&S takes to bolster election security. Every ES&S system we field undergoes rigorous testing by independent Federal test labs accredited by NIST. Since 2009, ES&S has certified 22 unique voting system releases through this Federal testing program. Our standard procedure is to conduct thorough and pervasive penetration testing of our hardware and software using the same modern security tools that hackers use to make sure our equipment is secure before it ever enters the Federal program. We recommend increased EAC funding for security testing managed at the Federal level with standards and testing methods that are applied evenly and comprehensively to all providers.

All ES&S tabulation firmware and software are not only housed domestically but are also written exclusively inside the United States. ES&S engages an independent third party to regularly test samples of the components inside our voting equipment that are programmable logic devices. We do this to validate the security of our supply chain and to ensure that no backdoor tampering has occurred. ES&S voting machine components are produced in ISO 9001 certified manufacturing facilities, and the entire voting system is managed by a secure engineering change order control process. All final hardware configuration of our voting machines is performed exclusively in Omaha, Nebraska.

We are working with our fellow industry providers seated with me here today to create the Nation's first coordinated vulnerability disclosure program for elections equipment, designed to provide for even greater independent testing of voting systems through the use of ethical hackers. Because we strive for continuous improvement in all facets of our business, our actions related to election security are continuous, ongoing, and dynamic.

Finally, I want to be clear that we do not believe we are perfect. On rare occasions, machines falter, and humans make mistakes. When these circumstances arise, we always do everything possible to remedy the issue and ensure that final election reports—results are reported accurately.

As I noted previously, we strongly urge Congress to require an auditable paper record for every vote cast as a matter of law to improve even more the integrity of our elections. While we are very proud of the actions we have taken to date in support of safe and secure elections, we recognize that this is a race that has no finish line. ES&S is committed to continually enhancing the security of our products for the long run. We take nothing more seriously than our role in supporting our Nation's democracy.

Thank you for your time, and I look forward to your questions.

[The statement of Mr. Burt follows:]

ES&S
ELECTION
Systems & Software

Statement from

Tom Burt
President and CEO of Election Systems & Software

Hearing on *"2020 Election Security –*
Perspectives from Voting System Vendors and Experts"

The Committee on House Administration
U.S. House of Representatives

January 9, 2020
Washington, D.C.

Chairperson Lofgren, Ranking Member Davis and Members of the Committee:

Thank you for the opportunity to testify on the vitally important subject of election security. My name is Tom Burt, and I am the CEO of Election Systems & Software. I am in my 12th year at ES&S and have served as the company's Chief Executive Officer for the last five years. I'm pleased to share with you today how ES&S provides services and products for use by our nation's elections officials, and I look forward to answering your questions. I am encouraged to see the growing attention to stronger security for elections and thank you for your support of ongoing improvement in this area. We recognize that the process of what makes elections work — including ballot design, voting, tabulating and certifying election results — is not always well understood by those who, unlike you and all of us on the panels today, live it every day. That's why I'm so pleased you're holding this hearing and giving us all an opportunity to share what we do and how we do it.

ES&S headquarters are in Omaha, Nebraska, where roughly half of our 490 employees reside and work. Other ES&S employees live in or near the states in which we provide services and products for our customers. In total, we have employees living in 39 of the 50 states. Our company began as a three-person "startup" roughly 40 years ago, focusing on developing a new way to apply scanning technology to aid counties that chose to tabulate precinct paper ballots at a central election office. Our unique application of this technology helped counties substantially improve the accuracy of initial vote counts and dramatically reduce the amount of time it took for jurisdictions to report results. We began with a single customer in Douglas County, Nebraska, and have grown steadily and mostly organically over time to become a leading provider of election products.

Our four decades of experience serving state and local jurisdictions have taught us that one size most certainly does not fit all. The methods of voting that are desired, or in some cases mandated, vary greatly from state to state and often from county to county. In response to these varied methodologies, ES&S has built our business on the foundation of customer satisfaction by tailoring our services and products to the extraordinarily varied needs and desires of the approximately 10,000 jurisdictions across the United States. Our customers have placed their trust in us time and time again over the last 40 years, and we are committed to continuing to earn their loyalty every single day. As part of that effort, ES&S has maintained a dedicated focus on reinvesting in our business through steady improvements in the quality of our personnel, products and services. Our ability to tailor our offerings to the unique needs of a given jurisdiction has enabled us to service and support major cities with millions of registered voters, as well as our smallest jurisdiction in Western Nebraska with fewer than 350 registered voters.

What never varies, however, is our commitment to ensuring that every vote is counted exactly as the voter intended. That's why I'm very proud to say that 22 unique ES&S voting system releases have earned federal approval from the Election Assistance Commission (EAC). In order to achieve a federal certification from the EAC, each voting system requires thousands of hours of testing and analysis. Additionally, our systems are evaluated against the best practices of the National Institute of Standards and Technology (NIST) security protocols and standards, as well as the Center for Internet Security's (CIS) Critical Security Controls. Every ES&S system we field undergoes rigorous testing by independent federally accredited test laboratories. We average more than $2 million in annual spending with these independent test labs alone in support of the certification process.

In light of cyber threats to our nation's elections ecosystem, we recognize the importance of a paper record, which is why ES&S was the first tabulation provider to ask Congress to pass legislation requiring an auditable paper record of every vote cast. This pillar of election security is so important to us at ES&S that we stopped selling voting machines that do not produce a tabulatable paper record as the primary voting device in any jurisdiction.

We took that step, and many more, because we believe there is nothing more crucial to upholding our nation's democracy than ensuring every vote is counted as cast.

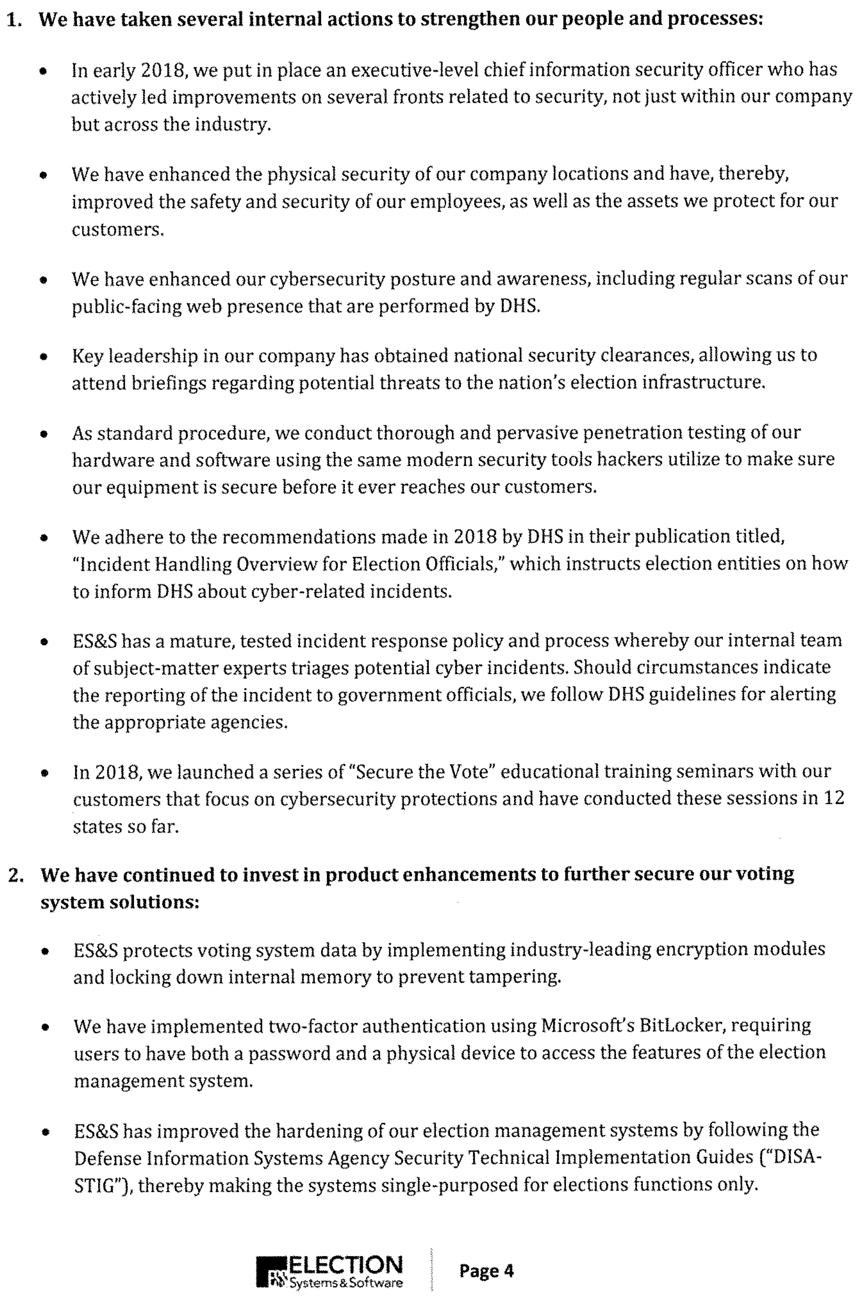
For more than a year, we have routinely met with members of Congress and their staff to discuss our products, services and commitment to election security, answering questions and providing information. To that point, last March, we drove several of our machines from Omaha to Washington, D.C., for a day-long demonstration of our products to all interested Members and staff. I led the briefing and was accompanied by our chief information security officer and several other senior company officials. This is all part of our ongoing effort to responsibly and actively engage with Members of Congress, the Department of Homeland Security (DHS) and other federal officials to improve election security.

Across the U.S., state and local jurisdictions have chosen to put in place more than 50,000 of our DS200 precinct-level paper ballot tabulation machines and more than 80,000 of our ExpressVote brand of universal voting machines. Every single one of our universal voting machines produces a paper record that can be tabulated and audited. Additionally, each of these machines enable a voter — including a voter with a disability, or a voter who is non-English speaking — to mark their ballot by touching a screen or using an assistive device, and the machine records that vote on paper. Before casting their ballot, the voter has the opportunity to review and verify their selections on that same piece of paper before it is cast as a vote. This paper record provides jurisdictions with the ability to audit every single cast vote and validate the integrity of the results for each election.

We acknowledge the growing concern among American voters regarding election integrity, and we support the increase in attention and dedicated resources coming from Congress, state and local officials, the EAC, and DHS. We embrace our partnerships with these bodies because we believe that collectively we can provide necessary and continuous improvement in election security. While the recent appropriations bill included additional funding from Congress, we believe the federal government needs to devote even more financial resources to jurisdictions that manage elections as part of the critical infrastructure in our country.

We view our role in helping to ensure election integrity with the utmost importance and are honored to do our part by providing elections officials with quality products and services for their use in conducting secure elections.

We have taken many important steps since 2016 to bolster the security of our voting solutions. We've organized these actions into four categories and note that while the list is long, it is only a sample of the many actions we've taken.



1. **We have taken several internal actions to strengthen our people and processes:**

    - In early 2018, we put in place an executive-level chief information security officer who has actively led improvements on several fronts related to security, not just within our company but across the industry.

    - We have enhanced the physical security of our company locations and have, thereby, improved the safety and security of our employees, as well as the assets we protect for our customers.

    - We have enhanced our cybersecurity posture and awareness, including regular scans of our public-facing web presence that are performed by DHS.

    - Key leadership in our company has obtained national security clearances, allowing us to attend briefings regarding potential threats to the nation's election infrastructure.

    - As standard procedure, we conduct thorough and pervasive penetration testing of our hardware and software using the same modern security tools hackers utilize to make sure our equipment is secure before it ever reaches our customers.

    - We adhere to the recommendations made in 2018 by DHS in their publication titled, "Incident Handling Overview for Election Officials," which instructs election entities on how to inform DHS about cyber-related incidents.

    - ES&S has a mature, tested incident response policy and process whereby our internal team of subject-matter experts triages potential cyber incidents. Should circumstances indicate the reporting of the incident to government officials, we follow DHS guidelines for alerting the appropriate agencies.

    - In 2018, we launched a series of "Secure the Vote" educational training seminars with our customers that focus on cybersecurity protections and have conducted these sessions in 12 states so far.

2. **We have continued to invest in product enhancements to further secure our voting system solutions:**

    - ES&S protects voting system data by implementing industry-leading encryption modules and locking down internal memory to prevent tampering.

    - We have implemented two-factor authentication using Microsoft's BitLocker, requiring users to have both a password and a physical device to access the features of the election management system.

    - ES&S has improved the hardening of our election management systems by following the Defense Information Systems Agency Security Technical Implementation Guides ("DISA-STIG"), thereby making the systems single-purposed for elections functions only.

- We have developed protections to ensure that each system we sell allows every voter the ability to review their printed vote selections before casting their ballot; a necessity for supporting risk-limiting audits.

- Our systems employ enhanced user access controls following the Principle of Least Privilege, so that user access is restricted only to the functionality that is required.

3. **We have increased our involvement and coordination with federal agencies and other vendors to improve security:**

- ES&S was the first tabulation provider to travel to East Greenbush, New York, to learn how the Center for Internet Security (CIS) assists in protecting elections, and subsequently became the first tabulation provider to join the newly created Election Information and Sharing Analysis Center (EI-ISAC) as a supporting member, allowing us to obtain – in real-time – the same information received by the nation's election officials regarding potential threats, as well as best practices.

- We are founding members of the newly created Election Special Industry Group (E-SIG), housed as part of the IT Information and Sharing Analysis Center (IT-ISAC), whose mission is to improve the safety of our voting systems. As a result, members help their companies improve their incident response through trusted collaboration, analysis and coordination. The group also helps drive decision-making by policymakers on cybersecurity, incident response and information sharing issues.

- ES&S leadership served as vice chair of the Sector Coordinating Council (SCC) during its inaugural year, dedicating countless hours to standing up the first-ever council of its kind for elections under the auspices of the nation's Critical Infrastructure Framework.

- ES&S currently continues in its leadership role in the SCC, with our chief information security officer serving as its current chair.

- During national general elections, ES&S has a physical presence in the situational awareness room hosted by DHS in Washington, D.C., which allows us to share information in real-time.

- We have participated in both annual DHS national tabletop exercises, and also invited DHS to Omaha, where they led a led tabletop exercise for employees at our company headquarters.

4. **ES&S works with recognized, independent experts in testing:**

- We have sought out and undergone independent third-party testing, including penetration and full security testing by the Idaho National Laboratory, performed in partnership with DHS.

- We were the first provider to work with DHS and CIS to put in place Albert sensors to monitor the platforms that we host for applicable state election offices. Albert is a unique network security monitoring solution that provides continuous remote monitoring and delivery of automated alerts regarding both traditional and advanced network threats for state and local jurisdictions, allowing election jurisdictions and ES&S to quickly respond when data may be at risk.

- ES&S' internal staff receives, evaluates and acts upon, as necessary, vulnerability reports received from software manufacturers, cybersecurity researchers and other third parties.

- ES&S engages an independent third party to regularly test samples of the components in our voting equipment that are Programmable Logic Devices (PLDs) – we do this to validate the security of our supply chain and ensure that no back-door tampering has occurred.

While the list is long, the actions are continuous, ongoing and dynamic. For example, we are actively participating — along with academics, election officials, federal agencies and the EAC — in the creation and formation of the most recent voting system test guidelines, the VVSG 2.0. Even though these standards have yet to be formally adopted, all our products are designed, without compromise, to meet the latest and ever-evolving principles in security, accuracy and reliability.

We strive for continuous improvement in all facets of our business, and we embrace our role as a leader in our industry. As I mentioned earlier, ES&S was the first provider to publicly state it will no longer sell a primary voting system that does not provide an auditable paper record. We strongly support post-election audits and believe that a true audit requires a physical paper record that can be both tabulated and subsequently audited. We support the EAC receiving the financial and administrative support needed from Congress to bolster the federal testing and certification program by conducting additional and more rigorous penetration testing of voting systems from all vendors who endeavor to service and support elections across America. This testing must become mandatory for elections providers and must be managed at the federal level with standards and testing methods that are applied evenly and diligently to equipment from all providers. Attached to this statement is a published op-ed I wrote that supports these suggested federal mandates.

Let me also be very clear that we do not believe we are perfect or invincible. On rare occasions, mistakes are made, a machine falters, or a human error is uncovered. Our reaction to any problems that occur is swift and comprehensive. Our record makes clear that working with the relevant local officials, we immediately seek to identify the potential problem, send in a team of experts to consult with the customer, and do everything possible to remedy the issue and ensure that final election results are reported accurately.

Our dedication to the protection of American's votes will not stop. We are working with our fellow providers, in conjunction with the IT-ISAC, to create the nation's first Coordinated Vulnerability Disclosure Program (CVDP) for elections equipment, designed to provide for even greater independent testing of voting systems using ethical hackers.

Our focus is equally sharp toward the protection of the individual components that make up our systems. A global supply chain is an economic reality for manufacturers in today's world. That's why ES&S partners with contract manufacturing companies who utilize DHS supply chain security programs such as the Customs-Trade Partnership Against Terrorism (CTPAT) program and the Authorized Economic Operator (AEO) program to support supply chain security. All final hardware configuration of ES&S voting machines is performed exclusively in Omaha, and all tabulation firmware and software are not only housed domestically but are also written exclusively inside the United States of America.

Product sustainability and stringent security controls are the driving force in maintaining a strong supply chain. We choose long-life industrial-grade components to ensure we maintain parts availability for the life of our products, which typically span a minimum of 10 years and often are in use for 15 to 20 years. ES&S voting machine components are produced in ISO-9001 manufacturing facilities, and the entire voting system is managed by a secure engineering change order control process. Every unit is individually serialized for complete traceability, and we conduct frequent audits and document proof that we are producing the product to its design specifications. ES&S involvement covers the entire product lifecycle, from the initial design to end-of-life.

While elections officials most certainly recognize the importance of each and every election, they know the significance of the 2020 general election and are working tirelessly to ensure a secure and trouble-free election. Our support of these election officials is essential to their success, as many of our customers either have recently installed or will be installing new equipment in advance of the upcoming election cycle.

To that end, this past November, millions of voters cast their ballots using new voting machines, marking a first-use for tens of thousands of pieces of equipment — the largest set of implementations since the Help America Vote Act was enacted in 2002. Last year, officials in nearly 150 jurisdictions nationwide installed new ES&S paper-based voting systems in advance of the November 2019 elections. In these jurisdictions, elections officials put in place more than 30,000 new fully accessible universal voting machines and more than 7,500 new precinct-level ballot tabulation machines.

While we are very proud of the actions we have taken to date in support of safe and secure elections, we recognize that this is a race that has no finish line. ES&S is committed to continually enhancing the security of our products for the long run. We take nothing more seriously than our role in supporting our nation's democracy.

Thank you for your time and attention.

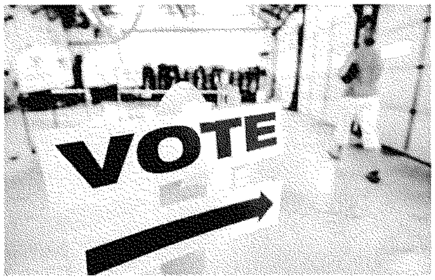
Roll Call

Jun 7, 2019

Opinion

A paper record for every voter: It’s time for Congress to act

Along with mandatory machine testing, it’s the only way to secure our nation’s democracy



OPINION — Over the last few years, policymakers, election security experts and voting equipment vendors have examined how we can continually ensure our elections and voting machines remain safe and secure.

Recently, we've seen many lawmakers — from bipartisan members of the Senate Intelligence Committee to presidential candidates — call for reforms to secure the integrity of our elections. When it comes to the machines that count votes and the people who make those machines, there are a few things that must happen to ensure faith in our system of democracy continues.

First, Congress must pass legislation establishing a more robust testing program — one that mandates that all voting machine suppliers submit their systems to stronger, programmatic security testing conducted by vetted and approved researchers. Voting machines may not be connected to the internet, but there are non-internet types of security testing necessary to protect elections.

Second, we must have physical paper records of votes. Our company, Election Systems & Software, the nation’s leading elections equipment provider, recently decided it will no longer sell paperless voting machines as the primary voting device in a jurisdiction. That’s because it is difficult to perform a meaningful audit without a paper record of each voter’s selections. Mandating the use of a physical paper record sets the stage for all jurisdictions to perform statistically valid postelection audits.

Third, let’s build on the elements of our nation’s voting infrastructure that are working well.

There are about 10,000 jurisdictions in America that manage nearly 117,000 polling locations and utilize more than 560,000 voting machines (manufactured by multiple suppliers) on Election Day. That’s what you call a highly distributed and differentiated infrastructure, which is great for security because it's virtually impossible for a bad actor, or even a troupe of bad actors, to attack on a large scale due to the complex differences across the nation.

Voting machines are, in fact, tested. Manufacturers submit their systems to the Election Assistance Commission, or EAC, which conducts lengthy testing and grants certification to those machines.

But we need to enhance federal- and state-level tests, which focus on functional and environmental testing, with further mandatory security testing. Machine penetration tests, for example, simulate attacks on election equipment by people who gain physical access to the voting machines or their components. Although elections suppliers and jurisdictions alike go to great lengths to physically secure election equipment, human beings still interact with these machines before, during and after Election Day. That means the machines must be secure enough to resist attacks at any point in the process.

Most voting system providers already voluntarily perform their own security testing or hire independent firms to do it — ES&S just submitted its equipment to the Idaho National Lab, which the Defense Department uses, for extensive penetration testing. But there is a clear need for the establishment of standards for machine penetration testing. That's what is missing and what needs to change.

If Congress can pass legislation that requires a paper record for every voter and establishes a mandated security testing program for the people making voting machines, the general public's faith in the process of casting a ballot can be restored. And that's not just a good thing, it's essential to the future of America.

Tom Burt is the CEO of Election Systems & Software.

http://www.rollcall.com/news/opinion/paper-record-every-voter-time-congress-act

The CHAIRPERSON. Thank you very much.

We'd be pleased to hear from you, Mr. Poulos.

TESTIMONY OF JOHN POULOS

Mr. POULOS. Thank you very much. Chairperson Lofgren, Ranking Member Davis, and distinguished Members of the Committee, thank you for the opportunity to testify today. My name is John Poulos, and I'm the Chief Executive Officer of Dominion Voting Systems. We are a U.S.-owned company that currently provides voting systems and services to jurisdictions across 30 States and Puerto Rico.

I agree with the importance of this—of the issues being raised by the Chairperson and Ranking Member regarding election security and integrity at today's hearing. American elections safeguard and preserve the freedoms and rights guaranteed by the U.S. Constitution. At Dominion, we take pride in our small role in assuring voters that they can have confidence in election results. We go to work every day understanding this important responsibility.

By way of background, I formed the company with my partners in 2003 as an engineer and entrepreneur living in Silicon Valley. We were one of 76 new entrants innovating in the post-HAVA era, and we are one of the only ones independently operating of those 76 in the industry today.

Dominion was founded on three key pillars: security, transparency, and accessibility. The company abides by these principles to this day, driving innovations and advancements for auditability and resilience directed by Federal, State, and local election officials.

Supporting elections is a full-time proposition for our company. This past year alone, Dominion assisted State and local election officials in conducting nearly 300 elections complete with the rigorous public scrutiny that comes with it. Dominion is constantly innovating and certifying enhancements and new features per State and local requirements. For 2020, we have been working closely with jurisdictions seeking to upgrade their voting systems. Older, end-of-life technology is being replaced with certified solutions that produce paper records for auditing and resilience. This comports with recommendations by DHS.

Consistent with our founding tenets, Dominion works hard to promote a company culture of security. This starts with our people, including annual mandatory background checks and cybersecurity awareness training for every employee in the company. It includes companywide adoption of advanced digital protections and a defense-in depth approach to cybersecurity. Moreover, we actively engage with the EAC, DHS, and other trusted third parties to maintain and enhance our enterprise security, including potential supply chain risks.

Finally, we meet all independent testing requirements, including EAC standards developed in conjunction with NIST and requirements set forth by individual States. This includes source code reviews, penetration testing, and post-election audits.

In terms of transparency, Dominion systems fully support independent third-party audits and reviews of all election data. For example, in 2018, the State of Colorado used Dominion systems in conducting the first statewide risk-limiting audit in the United States. This effort was so successful, it has become a benchmark for other States in verifying with high confidence that equipment tallies are accurate and reliable.

To round out our company mission, we are committed to voter accessibility. Our systems ensure Federal protections for privacy and equal voting rights and ballot casting options for all, including American servicemembers abroad.

The existence of nation-state threats means that we must actively defend against any attempts to undermine faith in our democratic institutions. In this regard, we hope to see Congress continuing its work with State and local election officials to keep election systems secure. We commend Congress on its bipartisan investment of an additional $425 million to help election officials modernize their infrastructure.

In closing, we remain fully committed to providing technology that supports free and fair elections. This includes support for an industry wide coordinated vulnerability disclosure program for voting systems. We urge you to continue supporting and incentivizing real-time threat information sharing from the intelligence community, streamline certification options for patching and updating, and reliable baseline security standards for voting systems. All of these efforts will help make the voting process more secure.

Thank you again for the opportunity to share our company's perspective.

[The statement of Mr. Poulos follows:]

Written Testimony of Mr. John Poulos, CEO

Dominion Voting Systems

before the Committee on House Administration

"2020 Election Security-Perspectives from Voting System Vendors and Experts"

January 9, 2020

Chair Lofgren, Ranking Member Davis, and Distinguished Members of the Committee, thank you for the opportunity to testify today.

My name is John Poulos, and I am the Chief Executive Officer and co-founder of Dominion Voting Systems. As a U.S.-owned company, we currently provide voting systems and services to jurisdictions across 30 states and Puerto Rico.

I co-founded the company in 2003 on three basic pillars: security, accessibility and transparency. We continue to be committed to these founding principles and delivering best-in-class solutions for secure, transparent, and accessible elections. The voting systems that we produce provide high assurance that election outcomes are accurately and reliably tallied. All Dominion systems fully-support independent, third-party audits, and reviews of election data.

Together with my industry counterparts, I am here today to help explain how we are working to keep voting systems secure and resilient in the wake of today's sophisticated, nation-state threats. I would like to focus on our core company values and how they impact our product innovations and the work that we do in collaboration with our federal, state, and local government partners.

Consistent with our founding tenants, Dominion works hard to promote a company culture of security. This includes annual, mandatory background checks and cybersecurity awareness training for all employees. Dominion is committed to investing in security and innovation efforts, tracking risk and threat information, developing new capabilities and successfully supporting our customers.

Dominion has also adopted advanced digital protections while employing a Defense-in-Depth approach to our internal infrastructure. Multiple layers of protection are in place spanning user endpoints, network and systems infrastructure and cloud systems, along with multi-factor authentication. We conduct continuous vulnerability scanning on our company network and utilize third-party services for threat hunting and breach detection. Specifically, we have implemented email verification records for Sender Policy Framework ("SPF"), DomainKeys Identified Mail ("DKIM"), and Domain-based Message Authentication ("DMARC") to protect communications with associates and customers.

We actively engage with the U.S. Department of Homeland Security ("DHS") and other trusted, third-party advisors to enhance and maintain our physical and cyber security posture. Together with federal, state and local government partners – as well as our industry counterparts, we conduct coordinated emergency drills, tabletop exercises and routine information-sharing as a member of the DHS Sector Coordinating Council for Election Infrastructure. Through these efforts, Dominion has refined our company's situational awareness and strengthened our procedures for handling incidents and emergencies.[1] We have also conducted security briefings and training sessions with state and local election officials who use our systems to educate and inform them of best practices for securing their voting equipment and chain of custody process. In these ways, we have made great strides to support and enhance the nation's collective readiness posture for the 2020 presidential election.

Dominion also works closely with jurisdictions seeking to upgrade or replace older, end-of-life systems with federally-certified solutions capable of producing paper records for auditing and resilience. These offerings have rigorous security features, and we provide hardware maintenance service and certified software/firmware updates on a routine basis.

In keeping with company security practices, all of our products are submitted to the U.S. Election Assistance Commission ("EAC") and state election authorities for further review, testing and certification. Systems are tested using an independent, federally-accredited Voting Systems Test Laboratory ("VSTL") in order to meet certification standards promulgated by the EAC, in conjunction with experts at NIST. They must also meet specific requirements set forth by individual states, including source code reviews, penetration testing, and post-election auditing.[2] These certified software packages and systems are the only versions allowed by law.

We are constantly innovating and certifying enhancements and new features, per federal, state and local election requirements. Our product advancements reflect the values of our state and local customers, with a focus on providing secure, reliable, quality systems that offer cutting-

[1] See U.S. Dept. of Homeland Security, "Incident Handling for Election Officials," 2018.

[2] Help America Vote Act of 2002 (HAVA). https://www.eac.gov/assets/1/6/HAVA41.PDF

edge features, including encryption, multi-factor authentication and trusted-user protections, as well as a robust auditing module for election officials who want to share post-election ballot images and other data with the public.

Dominion is actively engaged with the EAC and other stakeholders in the ongoing work to finalize VVSG 2.0 guidelines for 2020 and beyond. Our development strategy has shifted towards the latest iteration of these standards to ensure that our voting systems advance to the next generation of security and resilience. In 2018, Dominion equipment was used in the State of Colorado's risk-limiting audit ("RLA"), the first of this kind ever conducted in the U.S. Today, other states are conducting RLAs to ensure that election tallies are accurate and reliable.

Voting systems must also ensure federal protections for privacy, equal voting rights and ballot-casting options for all - including disabled voters, U.S. military and overseas voters, and those with literacy or language challenges who require some form of assistance in casting their ballot.[3]

Additionally, we are working with other industry companies to establish a Coordinated Vulnerability Disclosure ("CVD") program designed to strengthen the security and resilience of voting systems. This work expands upon existing federal and state processes for certification, testing and reporting on risks and vulnerabilities regarding election infrastructure. Government partners at all levels can help by supporting and incentivizing rapid modernization of the framework that is used for the certification and testing of election equipment.

Right now, the complex pathway from lab to market impacts the pace at which new or updated solutions can be introduced. While much of the current effort around VVSG has understandably focused on establishing thorough and comprehensive testing criteria for voting systems, there must also be clear mechanisms for streamlined updates and security-focused patching. We are hopeful that VVSG 2.0 will provide a more effective process for introducing innovations and maintenance of deployed systems.

Dominion makes extensive disclosures to maintain our good standing as a registered federal and state voting systems manufacturer. Like other providers, we submit a detailed "bill of materials" to the EAC as part of required submissions for federally-certified systems, which includes all component manufacturer and sourcing information for hardware. In addition to mandatory state and local disclosures for confirmed or suspected breaches and incidents, we also adhere to the

[3] See Americans with Disabilities Act, UOCAVA, Help America Vote Act (HAVA) and MOVE Act for specifics.

EAC's mandatory requirement for reporting system issues in federal elections.[4]

Federal and state-level product testing and certification applications require voluminous amounts of manufacturer information, including but not limited to:

- Ownership information, business structure and credit rating
- Notifications to all U.S. customers of any business change of ownership
- Personnel oversight policies, including background checks
- Third-party vendor and manufacturing location information
- Proprietary software disclosures, third-party test reports, and documentation to verify reliable use of the system in other jurisdictions

Dominion has always maintained full federal and state compliance under law. Given the high headline risk and the public visibility of the support that Dominion provides to state and local governments, it would be difficult to thrive as a business without maintaining the highest standards as an elections industry provider. Notably, voting systems manufacturers remain the only technology providers in the election ecosystem subject to company disclosures and federal certification testing. Only a handful of states currently extend their requirements beyond voting systems to other types of technology.

In conclusion, Dominion Voting Systems is committed to ensuring that Americans are confident in the security and resilience of the nation's voting systems. We commend Congress for its most recent bipartisan efforts to increase federal investment in state and local government election security initiatives for 2020 by $425 million. We urge you to continuing work with election officials to help remove additional barriers that exist for modernizing their infrastructure.

We also seek continued assistance from our federal partners in evaluating cyber risks for voting technology, to include increased transparency around malign activity observed by intelligence agencies. This would go a long way towards enabling private sector election providers to better prioritize resource allocations in the same economic terms as other enterprise decisions.

Dominion continues to focus on being the best-in-class elections provider with a commitment to security, transparency, and accessibility. Thank you again for the opportunity to share the company's perspective on these very important issues.

[4] See "EAC Testing & Certification Program Manual Version 2.0," www.eac.gov/assets/1/6/Cert_Manual_7_8_15_FINAL.pdf

The CHAIRPERSON. Thank you so much for your testimony.

And now our final witness on this panel, Ms. Mathis. We'd be pleased to hear from you for five minutes.

TESTIMONY OF JULIE MATHIS

Ms. MATHIS. Chairperson Lofgren, Ranking Member Davis, and Members of the Committee, thank you for the opportunities to speak with you today. My name is Julie Mathis, and I'm the CEO of Hart InterCivic. Hart InterCivic is based in Austin, Texas, where we have been located since our inception over a hundred years ago. Hart began as a paper ballot printer and over the past 20 years has grown organically one new customer at a time to become one of the top three voting system providers in the country. Our customers are local election officials, and our business is built on partnering with them every day to help solve their problems, enhance their processes, and ensure they deliver secure, accessible, and transparent elections.

Our products include the software and devices that these election officials use to create ballots, capture votes, tabulate votes, and audit the results. Our systems are regulated as each is submitted to Federal certification through the EAC as well as the State certification processes before any local jurisdiction purchases them.

It's also important to know which aspects of the election ecosystem Hart does not serve. Hart does not build the products that manage voter registration, voter check-in at the polling place, the public recording of election night results, or any other aspect of election or data administration. These aspects of the election system and their vendors are not currently regulated.

I am in Washington, D.C., this morning because Hart strongly believes that voting system companies are one of the many critical players ensuring American elections are accessible, transparent, and secure. I can tell you much has improved over the past few years for Hart and for the industry, but we know that challenges remain, and we must continue to evolve and adapt.

So what has improved? First, what has improved as a company is our products. We are proud that our Verity voting system is one of the newest and, we believe, most secure line of election products on the market. Rather than patch updates on older technology, Verity is a wholly new product designed from its core to meet modern security standards. Verity's robust security strategy is further described in my written testimony.

Second, what has improved as an industry? The election industry is far better informed, better supported, and more agile when it comes to cybersecurity threats as a direct result of the Department of Homeland Security's designation of the American election system as critical infrastructure. Because of that designation, we're a founding member of DHS' Sector Coordinating Council, a group of diverse elections-related vendors under DHS' stewardship to address resilience policies and practices. Similarly, we're a founding and engaged member of the ICS-ISAC as well as an active member of the EI-ISAC. All offer a range of valuable programs, free assessments, and educational materials, but the biggest improvements have been to our ability to community and coordinate around cyber threat information and disclosures.

So where else can we all continue to evolve and adapt? Number one, continual evolution of the voting system guidelines. We strongly support the process to roll out updated national standards. We have submitted our comments during the public comment period draft of the draft VVSG 2.0 and are in regular communication with the EAC to provide further insights to inform the new standard.

We share your frustration over the slow adoption of the new standards, yet Hart has proactively enhanced the security of our products while awaiting the release of the 2.0 standards. In addition, we encourage Congress and the EAC to continue to explore ways to apply Federal oversight to other election technology, especially areas of higher vulnerability, such as voter registration, electronic pollbooks, and election night results reporting.

Number two, speed up the Federal certification process at the EAC. We are optimistic that Congress' recent increase in funding may allow additional resources to be dedicated to the ongoing overhaul of the VVSG and to enhance certification of resources at the EAC. The more resources and funding that Congress can dedicate to the EAC and NIST, the sooner we will be able to bring the next generation of products to market.

Number three, ongoing vigilance over cybersecurity practices within our companies and within local jurisdictions. The most important shift in institutional attitudes towards securing the integrity of election systems is that security is not a static process. At Hart, we recognize that cybersecurity threats will evolve, and so we, along with local jurisdictions, must continually adjust to new risks and adapt with new technology, new processes, and new policies.

In conclusion, much has improved over the last few years. Not only are there new products on the market with enhanced security protocols, but the election industry is much better informed, more coordinated, and more aware. But this enhanced awareness also highlights the clarity that securing the American election system is a race with no finish line. It will take constant vigilance, funding, partnership, and coordination across all aspects of the election ecosystem to ensure that elections are secure each and every year.

At Hart, our goal is and always has been to provide election officials with accessible and secure technology. We dedicate significant time and resources, ensuring our products meet or exceed the latest security standards. And because of this, we are a trusted partner of the local officials who run elections in our country.

Thank you, and I look forward to answering any questions you may have.

[The statement of Ms. Mathis follows:]

Statement for the Record

Julie Mathis
President and Chief Executive Officer
Hart InterCivic, Inc.

HART
intercivic™

For a hearing on
2020 Election Security:
Perspectives From Voting System Vendors And Experts

Before the
U.S. Committee on House Administration

January 9, 2020

Chairperson Lofgren, Ranking Member Davis, and members of the Committee, thank you for the invitation and for the opportunity to speak with you this morning about recent steps the election industry has made to better secure the integrity of the American election system. My name is Julie Mathis and I am the CEO of Hart InterCivic.

Hart InterCivic is based in Austin, Texas where we have been located since our inception over 100 years ago. Hart began as a paper ballot printer and, over the past 20 years, we've grown organically – one new customer at a time – to become one of the top three voting system providers in the country, with customers across 20 states. Hart's voting systems are designed, engineered, and built in the United States. In fact, our manufacturing plant is only a few short miles from our headquarters in Austin, allowing us to carefully monitor the entire build and testing process end-to-end. Because we value transparency, we have invited state and local election officials from around the country, as well as officials from the Department of Homeland Security (DHS) and the Election Assistance Commission (EAC) to tour our manufacturing plant to see where and how our devices are manufactured.

At Hart, we build the voting systems that local election officials use to create ballots, capture voter choices, and tabulate and audit results. And because the elections industry is broad, it's also important to note what elements of the election process we do not provide: Hart does not manufacture any products or provide services that manage voter registration, voter check-in at the polling place, the public reporting of election night results, or any other aspect of election or data administration.

I traveled to Washington DC to participate in this hearing because Hart strongly believes that voting system companies are one of the many critical players that ensure that American elections are accessible, transparent, and secure.

I will provide perspective on a few key aspects of how the election industry has adapted to meet new challenges and threats. I'm excited to discuss how Hart as an individual company has continued our focus on security, as well as how our engagement in the larger election community has made the entire industry more secure. Much has been done by members of this community, and we are committed to continue to evolve and adapt to the changing landscape.

- The national election system is far more secure and the officials responsible for managing it are better prepared to thwart cyber security attacks today than ever before, thanks in large part to the designation of the American election system as "Critical Infrastructure" by DHS.
- Hart and the other companies present today – along with many companies not represented at this hearing – are proactive in our approach to security. We're constantly learning and improving our protocols through our engagements with federal security agencies and security experts. We're not waiting around to make our products, our company, and our customers, local election officials, more secure – we do that every day.
- Strong leadership from organizations like DHS, the National Association of Secretaries of State (NASS), and the National Association of State Election Directors (NASED) has delivered needed attention and resources to election offices across the country.

Critical Infrastructure

The election industry is better informed, better supported, and more agile when it comes to cyber security threats as a direct result of DHS' designation of the American election system as Critical Infrastructure after the 2016 Presidential Election.

We saw the value in engaging with DHS immediately and so became a founding member of its Sector Coordinating Council (SCC), a group of diverse elections-related vendors that have come together under DHS's stewardship to address sector-specific resilience policies and practices, as well as to share threat information across the industry. Similarly, we are a founding and engaged member of the IT-ISAC (EI-SIG)[1], as well as an active, non-voting member of the EI-ISAC [2] (full, voting membership in the EI-ISAC is reserved for state and local election officials only).

The SCC and the ISACs, both available to the industry only because of the designation of Critical Infrastructure, enable election officials and industry representatives to interact on a wide range of sector-specific strategies, policies, and activities. Though both offer a range of valuable programs and educational materials, the biggest impact has been to our ability to communicate and coordinate around cyber threat information. Prior to the designation of Critical Infrastructure, the election community had little guidance and no direct portal to report and share information on potential vulnerabilities or discovered cyber security threats.

Today, our ability to share information across the industry has drastically improved. Both DHS and the ISACs provide dedicated lines of communication for the reporting of any new threat information up to the national intelligence agencies and then across the entire industry in a matter of hours. Typically, the information shared is related to suspicious IP addresses and phishing campaigns, but the industry stands ready to act on more serious attacks. Additionally, both DHS and the ISACs offer free security-related programs and services such as briefings on foreign threat tactics and practices, cyber security assessments, and best practice guides and checklists on election security.

The effect these groups have had on our industry in just a few short years has been significant. Perhaps the best example of the real-world impact of the SCC and ISACs is the widespread adoption of coordinated vulnerability disclosure (CVD) programs across our industry. Through our participation in the IT-ISAC, we were able to meet and discuss CVDs with companies in other sectors of Critical Infrastructure and learn from their experiences. We then put that new knowledge to use immediately, calling on experts in the field to educate the industry on how CVD programs and "bug bounty" programs could be adapted to the field of voting system manufacturers. That discussion is on-going with the release of a white paper and a Request for Information (RFI) published by the IT-ISAC, but, in the meantime, we aren't waiting. Hart has implemented a dedicated line for ethical hackers to privately and securely report any perceived vulnerabilities in our products or our networks.[3]

[1] IT-ISAC (EI-SIG): Information Technology – Information Sharing and Analysis Center (Elections Industry – Special Interest Group)

[2] EI-ISAC: Election Infrastructure – Information Sharing and Analysis Center

[3] To date, Hart has not received any reports through our CVD program.

Standards and Certification

The election industry is sometimes described as "unregulated," but that label, at least as it applies to Hart and our Verity Voting system, is misleading. Every voting machine we produce is designed to meet or exceed federal and state certification requirements.[4] After thorough internal testing, our systems are rigorously tested by independent, federally approved test labs. Despite the name of the federal standard – the Voluntary Voting System Guidelines (VVSG) – at Hart, we consider the VVSG to be anything but *voluntary*.

We strongly support, and are very actively engaged in, the process to roll out updated national standards that better address modern security practices. We have submitted comments during the Public Comment period of the draft VVSG 2.0 and are in regular communication with the EAC to provide insight and information that may inform the drafting of the updated standard. We share Congress' and election officials' frustration over the slow adoption of the new standards, and Hart has proactively continued to enhance the security protocols of our products, to ensure that we are not stagnant on critical security enhancements while waiting on the final release of the standards.

Further, we encourage Congress and the EAC to continue exploring ways to apply federal oversight on all election technology, including areas of high vulnerability – such as voter registration, electronic pollbooks, and election night results reporting.

We are optimistic that your recent increase in funding to the EAC may allow additional resources to be dedicated to the on-going update of the VVSG. As vendors, we can support and inform the process, but ultimately it is the EAC and the National Institution on Standards and Technology (NIST) that drive the program. The more resources and funding that Congress can dedicate to the EAC and NIST, the sooner we will be able to submit innovative new systems built to a more modern standard.

Hart InterCivic and the Verity Voting System

The most important shift in institutional attitudes toward securing the integrity of election systems is that security is not a static process. At Hart, we recognize that cybersecurity threats will evolve and so we must continuously adjust and adapt to new technology and new adversaries.

In recent years, we have actively and repeatedly revisited our own corporate business policies to ensure they are compliant and fully mapped to relevant national security standards, such as the NIST Cybersecurity Framework and the Center for Internet Security's Controls. All Hart employees must pass background examinations, and all employees go through repeated cyber security trainings and receive regular cyber security updates.

We are proud that our Verity Voting system is one of the newest and, we believe, most secure line of election products on the market. Rather than patch updates on to older technology, Verity is a wholly new product designed from its core to meet modern security standards.

[4] Not all states have their own state-specific certification program. Some states rely exclusively on certification to the federal VVSG, while others have their own robust certification standard independent of the VVSG.

Verity Voting systems incorporate a well-defined, end-to-end, defense-in-depth (multi-layer) security strategy across all software and hardware elements:

- Verity software cannot be accessed remotely, by Hart or anyone else.
- Verity does not encode voter selections in bar codes.
- All election data is secured with National Institute of Standards and Technology (NIST)/Voluntary Voting System Guidelines (VVSG)-compliant Federal Information Processing Standards (FIPS) 140-2 cryptography.
- Verity devices apply "surface attack reduction" in both the hardware and software to eliminate unneeded components from the voting device. Only the minimally required operating software and hardware components are built into the devices.
- Multiple, redundant data backups protect against data loss and provide comparisons to test against attempted data manipulation.
- Verity systems run in "kiosk" mode, which limits users' access to only those elements of the system they are authorized to use. No user has access to operating system files, and no other programs or files can be loaded onto systems or devices running Verity software.
- Verity devices employ "secure boot" methods that provide strong tamper notification of changes to the operating system or systems software.
- Verity employs "whitelisting" security which is more secure than traditional anti-virus applications. Whitelisting prevents any and all unauthorized software from running on the voting system.
- Verity election management software requires two-factor user authentication.
- Verity devices are protected with physical locks and tamper-evident security seals. Voters cannot insert external cards, drives, devices or cables as all external ports are protected through hardware obfuscation (non-standard connections).
- Verity tracks every user action, including logins, data entry, ballot resolution steps and other system events, providing comprehensive, plain-language audit logs that make it easy for all stakeholders to monitor how the system is used.
- Verity supports the most thorough and sophisticated post-election auditing to provide complete transparency into the accuracy of election results.
- Hart systems are designed, engineered and manufactured in the United States of America, right in our hometown, Austin, Texas.

Even with all the security features listed above, we recognize that election security requires more than applying modern technology with the latest tools and protocols. It also requires properly trained election staff using well-defined processes. Hart assists our customers in conducting secure elections by providing thorough training on all aspects of the system and by sharing best practices for processes such as managing and documenting equipment chain-of-custody and using and logging physical security seals.

We also provide instructions and training in conducting tests to validate our customers' voting systems are operating properly throughout the ownership lifecycle. Tests include user acceptance testing, logic and accuracy testing prior to each election, and parallel testing to ensure the system performs as required, and post-election audits to assure stakeholders that results are accurate.

In the election industry, the relationship between vendor and election official is a long-term partnership. The initial point of sale of an election system is only the introduction to what are typically decade-long relationships. In addition to providing technology, Hart stays in constant contact with our customers through newsletters, calls, emails, regular visits, and webinars to help ensure we are sharing the latest intelligence and best practices regarding election security.

Supply Chain

Protecting the integrity of elections is at the core of everything we do and securing our supply chain is a responsibility we take seriously. Our efforts include protection of our manufacturing operations, assessment of points of origination of all components of our products, safe-handling protocols, tracking of inventory, secure container locks and tags for products in transit, and monitoring of both external and internal risks to technology and data. We use only trusted partners in our manufacturing supply chain, and ensure that our supply chain is fully mapped, controlled and monitored from design through final delivery of a device. We actively monitor and log all chains of custody. The supply chain is regularly reviewed for new risks and our policies are continuously updated or enhanced to address any new vulnerabilities.

Though responsibility for the physical storage and conservation of election equipment rests with the local election offices once delivered, at Hart, we know our role in safeguarding those devices continues. Hart routinely provides services and education to our customers to improve security practices even after the final delivery of our products. For example, Hart regularly releases best practice recommendations and even provides in-person training with our experts on how to securely and efficiently warehouse voting systems in their government facilities. Election security experts refer to the importance of cultivating secure election management through a combination of "people, processes, procedures and technology," and Hart provides specific guidance to customers regarding the necessary security protocols to maintain ongoing security at every one of their election sites.

Conclusion

Hart remains dedicated to supporting our customers as they conduct smooth, issue-free elections which translate into high levels of voter confidence. Our systems are:

- Fully accessible by all voters, including those with disabilities, without sacrificing security.
- Capable of supporting the most sophisticated audits for full transparency.
- Federally and state certified, including thorough, independent laboratory testing.

In my perspective much has improved over the last few years – not only are there innovative products on the market with enhanced security protocols, but the election community is much better informed, more coordinated, and more aware. But this enhanced awareness also highlights the clarity that securing the American election system is a race with no finish line. It will take constant vigilance, funding, partnership, and coordination across all aspects of the election eco-system to ensure that elections are secure each and every year.

Your recent allotment of $425 million in funding was a good start, but election officials need a regular supply of funding to improve the resiliency of their systems and purchase newer, updated voting machines.

I encourage Congress to maintain your oversight and continue to fund DHS, the EAC, and all the programs and tools they make available to election officials and election manufacturers. As you've heard today, those resources and tools are vital to our national security, and they are being implemented across the nation.

At Hart, our goal is, and always has been, to provide election officials with accessible and secure technology. We listen when experts release new best practices on cyber security. We engage in the national dialogue on election security. We participate in disaster preparedness exercises hosted by DHS and state election offices. We dedicate significant time, energy, and resources to ensuring our products meet or exceed the latest security standards. And because of all of this, we are a trusted partner of the local officials who run elections in our country.

Thank you for the opportunity to address the Committee on these important issues.

The CHAIRPERSON. Thank you very much, and thanks to all of our witnesses for your verbal testimony as well as your written testimony.

We'll now go to the time in our hearing where Members have an opportunity to ask questions for as long as five minutes, and I'll start.

We all know and recognize that concern about election security has been heightened since the 2016 election—we've had reports from our intelligence community that we should be on the alert for threats, especially foreign threats to the security of our systems. Right now, there are no Federal reporting requirements that mandate disclosure of crucial information about some of your key business practices or experiences. And I'd like to know from each of you, and this is going to be a yes-or-no question, would you support requirements concerning the following five items: first, your cybersecurity practices, including incident response procedures; two, any cyberattacks you've experienced; three, personnel policies and procedures, including whether background checks and other procedures are in place to safeguard against inside attacks; four, details of corporate ownership and foreign investment; and, finally, supply chains, for example, where parts, software patches, installations come from, how they're transported, and how they are kept secure? Would you—if you could answer whether you would agree to all, or if there are some that you would object to, why?

Mr. BURT. Madam Chairperson, I would say yes, that we would support a requirement for all five of those requirements that you listed.

The CHAIRPERSON. Thank you.

Mr. POULOS. Madam Chairperson, we would agree with that as well.

The CHAIRPERSON. Thank you.

Ms. MATHIS. As would we.

The CHAIRPERSON. That's very helpful. As you know, we have passed a pretty robust bill in the House that's pending in the Senate, and perhaps your testimony will encourage them to move forward.

I'd like to talk about supply chains. As I mentioned in my opening statement, the concern has been raised about components. The Enteros report showed that a majority of suppliers within a widely used voting machine supply chain had locations in either Russia or China. They didn't indicate which company. So I'd like to ask each of you. Do you have components in your supply chain that come from either Russia or China?

Mr. BURT. Madam Chairperson, we do not have components that come from Russia. We do have a limited number of components that come from China.

The CHAIRPERSON. What percentage would that be?

Mr. BURT. I can't give you a percentage, but with respect to this issue, the potential for a backdoor threat really doesn't pertain to inert items like a piece of plastic or a piece of metal. What we really should be concerned about are the programmable logic devices.

The CHAIRPERSON. What type of components come from China? Can you tell me the nature of the components?

Mr. BURT. Sure. I'll give you one example. Our DS200, which is a——

The CHAIRPERSON. Well, no. I don't want examples. Do any of your chips or software come from China, or are the Chinese components just pieces of plastic?

Mr. BURT. In our DS200, we have one of the nine programmable logic devices that we actually source from a U.S. company based in Milpitas, California, in the heart of Silicon Valley that produces that programmable logic device in a—in a factory in China.

The CHAIRPERSON. Okay. Thank you.

Mr. POULOS. Thank you for the question. It wasn't our company in Enteros' report, but we do have components in our products that come from China, and I don't know the exact percentage. I can certainly get that to the Committee through my staff. Happy to work with you on getting the exact number. Our products—our tabulated products have always been manufactured in the United States, and so if you look at——

The CHAIRPERSON. Well, can you—before you go forward, what are the components that you get from China?

Mr. POULOS. So, for example, LCD components, the actual glass screen on the interface down to the chip component level of capacitors and resistors. Several of those components, to our knowledge, are not even—there's no option for manufacturing of those in the United States. We would welcome guidelines and best practices from the Committee and from the Federal Government in terms of this is not a problem that's unique to the election industry.

The CHAIRPERSON. Thank you.

Ms. Mathis.

Ms. MATHIS. Yes. Similar feedback here. We take the security of our supply chain very seriously, and we actively monitor and assess all aspects of that supply chain, including country of origin.

The CHAIRPERSON. So do you have components from China or Russia?

Ms. MATHIS. We do not have components from Russia, but we do have—similar to my colleagues, we do have components from China.

The CHAIRPERSON. And what would be the nature of those components?

Ms. MATHIS. Similar: resistors, capacitors. They're the global supply chain for technology components for that——

The CHAIRPERSON. And what percentage, do you know?

Ms. MATHIS. I don't have that.

The CHAIRPERSON. We'll follow up with that.

I'll turn now to Mr. Davis for his five minutes.

Mr. DAVIS of Illinois. Thank you, Madam Chairperson, and thank you again to the witnesses who are here. Each of you, just a simple yes or a no. Is there any method of voting that's a hundred percent secure?

Mr. BURT. No.

Mr. POULOS. No.

Ms. MATHIS. No.

Mr. DAVIS of Illinois. To your knowledge, has a foreign state ever successfully breached or hacked any of your vote tallying election machines? Mr. Burt.

Mr. BURT. No.

Mr. DAVIS of Illinois. Mr. Poulos.

Mr. POULOS. No.

Ms. MATHIS. No.

Mr. DAVIS of Illinois. What, then, was the primary target of our foreign adversaries in the 2016 election? Mr. Burt.

Mr. BURT. Well, Ranking Member, I think there are potentially differing public views on that, but what I can say is that, as you asked a minute ago, we've seen no evidence that any of our voting systems have been tampered with in any way.

Mr. DAVIS of Illinois. Mr. Poulos.

Mr. POULOS. I would agree with that statement. We feel the same way. I can't speak to what the primary purpose was of the attacks, but there's, to our knowledge, no evidence on our systems as well.

Mr. DAVIS of Illinois. Well, you guys already answered that.

Ms. Mathis, do you know what was attacked during 2016?

Ms. MATHIS. I do not have personal awareness of that.

Mr. DAVIS of Illinois. Okay. I believe reports say there were centralized voter registration systems, even one in my home State of Illinois. Where do these centralized State voter registration system databases come from?

Mr. BURT. Ranking Member, they—it's various, depending on——

Mr. DAVIS of Illinois. Do they come from any of your companies?

Mr. BURT. We do host voter registration systems for a limited number of States, yes.

The CHAIRPERSON. How about you, Mr. Poulos?

Mr. POULOS. We do not.

Ms. MATHIS. We do not.

Mr. DAVIS of Illinois. Okay. They're actually a requirement in the Help America Vote Act.

And, also, Mr. Burt, to your knowledge, are there any parameters within HAVA that require basic security around the State voter registration databases?

Mr. BURT. I believe the language in HAVA as it relates to voter registration is limited at best, and I'm not aware offhand of any specific language that pertains to——

Mr. DAVIS of Illinois. Great. And I'll stick with you because you're the only one that actually deals with centralized voter registration, and the other two do not. Do you find this concerning and believe it's something that we should address in HAVA?

Mr. BURT. I do. I think it's a gap in the oversight of the election administration or Election Assistance Commission, and I believe you could put electronic pollbooks into the same bucket with voter registration.

Mr. DAVIS of Illinois. Okay. Are you members of the Sector Coordinating Council?

Mr. POULOS. Yes.

Ms. MATHIS. Yes.

Mr. DAVIS of Illinois. Okay. As well as the IT–ISAC and the EI–ISAC?

Mr. BURT. Yes.

Mr. POULOS. Yes.

Mr. DAVIS of Illinois. Okay. How have these entities increased vulnerability disclosure? Mr. Burt.

Mr. BURT. You know, prior to 2016, there was virtually no communication between vendors and those entities, and there is regular sharing of information, threat information as well as routine meetings, many face-to-face, to make sure that the lines of communication are open at all times.

Mr. DAVIS of Illinois. Okay. Mr. Poulos, how many different vulnerability disclosure programs are there currently?

Mr. POULOS. To my knowledge, we're part of one and currently working on several more with my colleagues here to create further disclosure programs.

Mr. DAVIS of Illinois. Okay. Ms. Mathis, how do we ensure that these new programs are adequate to disseminate known vulnerabilities to those that need to know?

Ms. MATHIS. I think it's important that we continue to work together with cybersecurity experts that have already been involved through the designation as critical infrastructure. It's really assisted us with ensuring that we understand kind of the appropriate disclosures.

Mr. DAVIS of Illinois. Would you all agree that there are a lot more people, both in the media and public interest groups and Congress, for that matter, writing on the topic of election security since the 2016 election?

Mr. BURT. Yeah.

Mr. DAVIS of Illinois. Would you all agree?

Mr. POULOS. Yes.

Mr. DAVIS of Illinois. I'm actually happy for this increased attention. I believe it's put an important issue to the forefront. I'm concerned about the incentive for outside groups to mischaracterize the threats facing our elections. Is this a concern that each of you share?

Mr. POULOS. Yes.

Mr. DAVIS of Illinois. I got one yes.

Mr. BURT. Yes.

Ms. MATHIS. Yes.

Mr. DAVIS of Illinois. Thank you. I didn't think C–SPAN could see you guys nodding your heads.

Ms. MATHIS. Yes.

Mr. DAVIS of Illinois. Over the past several years, DEFCON has garnered a lot of publicity. Have any of you reached out to DEFCON to participate?

Mr. BURT. Ranking Member, we have had discussions with them, but we have not provided our equipment to them for testing.

Mr. DAVIS of Illinois. Okay.

Mr. Poulos.

Mr. POULOS. Ranking Member, we reached out to DEFCON this year in 2019, interested in a more collaborative penetration testing with stakeholders. We reached out with one organizer and had a plan. We actually did send our modern certified equipment to DEFCON, but in the days leading up to that event, I think that there was an internal disagreement within the conference. So we ended up not working at that conference, but if it's——

Mr. DAVIS of Illinois. Okay.

Mr. POULOS [continuing]. Not DEFCON, we're committed to that.

Mr. DAVIS of Illinois. How about you, Ms. Mathis?

Ms. MATHIS. We have actually submitted our systems through the DHS' penetration testing process through Idaho National Labs, so we've—we've gone that route.

Mr. DAVIS of Illinois. But not DEFCON.

Ms. MATHIS. Not DEFCON.

Mr. DAVIS of Illinois. Okay. Thank you. I yield back.

The CHAIRPERSON. The gentleman yields back.

I now recognize the gentleman from Maryland, Mr. Raskin, for five minutes.

Mr. RASKIN. Madam Chairperson, thank you very much.

The Consumer Product Safety Commission advises manufacturers of consumer products to identify all reasonably foreseeable hazards associated with use of their products and to include safety warnings and steps to reduce risk of accident in the user guides. And there are requirements like this for motor vehicles and warnings put in lots of different owner manuals. Would you support a requirement for voting system vendors to identify security risks associated with use of your voting equipment and recommendations for users to mitigate those risks, such as manual audits of paper ballots? And just go down the line. Mr. Burt, we'll start with you.

Mr. BURT. Thank you, Congressman. We would support that. And as a global comment, I think we would support any requirement that applies to all vendors in our industry that would help educate both the users of our systems and anyone who interacts with them.

Mr. RASKIN. Thank you.

Mr. POULOS. Congressman, I would agree with that statement as well. We would support any initiative that Congress puts forward.

Mr. RASKIN. Okay.

And Ms. Mathis.

Ms. MATHIS. And we agree also with that.

Mr. RASKIN. All right. Very good. There has been some reporting recently about the lobbying practices of election—of technology vendors in the election field. The City Controller in Philadelphia issued an investigative report that showed serious flaws in the voting system procurement process, which I think resulted in ESS getting the $29 million contract. The reports indicate that ES&S spent $425,000 lobbying city officials dating back to 2013 before being awarded the contract. Is this just standard practice in the industry and with your business, Mr. Burt?

Mr. BURT. Well, Congressman, starting about a year and a half ago, we actually hired our first ever Federal consultant to help us spend time in Washington educating Federal officials on who we are as a company, how we go about our business practices. We use consultants at the State level for the same purposes, to educate decisionmakers.

Mr. RASKIN. Well, in this case, it was used to help procure a contract, right?

Mr. BURT. It was used to educate any of those involved about who we are as a company, the values we hold, and how we conduct our business.

Mr. RASKIN. Okay. Do you also get involved in making campaign finance contributions or expenditures?

Mr. BURT. No, we do not.

Mr. RASKIN. Okay. Mr. Poulos, do you guys engage——

Mr. POULOS. No, we don't make campaign finance contributions.

Mr. RASKIN. You do spend money on the lobbying side?

Mr. POULOS. Yes, we do.

Mr. RASKIN. At the State and local level?

Mr. POULOS. Correct.

Mr. RASKIN. Okay.

And Ms. Mathis.

Ms. MATHIS. Our involvement in lobbyists has been very minimal and primarily related to helping educate us on local procurement processes within certain jurisdictions.

Mr. RASKIN. Okay. I'm curious about whether each of your companies engaged in adversarial testing of your voting systems.

Mr. POULOS. do you——

Mr. POULOS. We have in the past. It's something that we're looking to expand in the future.

Mr. RASKIN. Okay. Mr. Burt.

Mr. BURT. We do routinely. We've hired third parties to perform penetration testing as Ms. Mathis mentioned earlier. We also participated through a DHS program with the Idaho National Lab to perform penetration testing on our equipment.

Mr. RASKIN. Okay. And Ms. Mathis.

Ms. MATHIS. Yes, and we have been involved in that same penetration testing approach by the DHS' recommended Idaho National Labs.

Mr. RASKIN. Okay. So do you routinely allow academic researchers to test the quality and security and integrity of your products without prescreening them? In other words, do you generally permit outside investigators to come in check it out?

Mr. BURT. We have not involved academics who haven't been prescreened. With the coordinated vulnerability disclosure program that we're working on with our colleagues, the idea is to have a firm be able to manage a network of white hat ethical hackers to broaden the access to our systems without making this information open to the public.

Mr. RASKIN. Okay.

Mr. Poulos.

Mr. POULOS. Congressman, we have done that in the past, as far back in New York in 2009. We found that the exercise was useful, and we are looking forward to doing more of that within the confines of a reality-based scenario of testing.

Mr. RASKIN. Okay.

And Ms. Mathis.

Ms. MATHIS. And we would support the appropriate disclosure of that information. It's important that we not undermine voter confidence in ensuring that we actually evaluate and assess kind of the type of disclosures necessary.

Mr. RASKIN. Okay. And, finally, I remember from my days in Annapolis that there was sometimes conflict between the disability rights community and the champions of security in the process.

And I wonder, Mr. Poulos, will you just try to illuminate that, if you could?

Mr. POULOS. Sure. Most recently, with a lot of the public commentary around ballot marking devices, there is a concern regarding the formality of how the ballots are printed for voters as the voter record, and that sometimes is a natural conflict between universal accessibility and security initiatives.

Mr. RASKIN. I yield back.

The CHAIRPERSON. The gentleman's time has expired.

The gentleman from will North Carolina, Mr. Walker, is recognized for five minutes.

Mr. WALKER. Thank you. Thank you, Madam Chairperson.

I believe each of you mentioned in your written testimony frustration with the voluntary voting system guidelines update that is ongoing at the Elections Assistance Commission. This frustration has been shared by others in the election industry, as well as this issue seems to have a lot to do with antiquated HAVA or Help America Vote Act. Where can we as a Committee focus to help update the HAVA?

I'll start with you, Mr. Burt.

Mr. BURT. Thank you for your question, Congressman.

I think that the EAC, given the resources and funding they have, do a very good job. And sometimes it amazes me how much they are able to accomplish given the resources they have. I think we should ask them to broaden the scope and purview of their oversight, and to do that, of course, they need more funding and more support.

Mr. WALKER. Okay.

Mr. Poulos.

Mr. POULOS. I would—I would agree with Mr. Burt's comments, and I would add to that a particular example as it pertains to patching specifically of third party software, such as Windows, where a patch is readily available, and it's sometimes very cumbersome and timely to get that tested patch to end customers.

Mr. WALKER. Thank you.

Ms. Mathis, anything to add to that?

Ms. MATHIS. I would agree with those comments.

Mr. WALKER. Okay. All right. How has your relationship with the DHS evolved? How have State and local authorities responded to DHS? I'll put up a couple of these, and who wants to take it? Is DHS helping to secure foreign supply chains? And what type of services does DHS currently offer you?

Mr. Poulos, let me start with you. Let's start with what type of services does DHS currently offer you?

Mr. POULOS. It offers several different programs. We've taken part of a physical security review. They offer product testing. And in terms of the evolution of that relationship, I would say it was zero 4 years ago, and it's been very helpful for not only us but the customers we serve.

Mr. WALKER. Mr. Burt, is DHS helping you to secure foreign supply chains?

Mr. BURT. They are not, and I think that's a real opportunity whether it's through DHS or Department of Defense or somewhere else in the Federal Government. As Mr. Poulos mentioned, I think the vendors are eager to work in partnership with the Federal Government to make sure that we're following best practices and we safeguard to the best of our abilities our Nation's voting equipment.

Mr. WALKER. Just reiterating this again, in working with DHS, as well as your own companies, any evidence that China or Russia has hacked any portion or part of this, either has the DHS discovered any of that or assumed or even suggested that, or anything of those nature?

Mr. BURT. No. We've never—we've never received any evidence or even commentary that suggests that these systems have been hacked.

Mr. POULOS. No. No.

Mr. WALKER. Ms. Mathis.

Ms. MATHIS. No.

Mr. WALKER. I've got a question here, and if you can expound a little bit on this. Have each of you hired an executive level chief information security officer? Mr. Burt.

Mr. BURT. We have.

Mr. WALKER. Mr. Poulos.

Mr. POULOS. We have.

Mr. WALKER. Ms. Mathis.

Ms. MATHIS. We have an extended internal security team, and we have a CISSP expert on our staff.

Mr. WALKER. Mr. Poulos, what are the qualifications for such a position? What are the requirements of that? What are you looking for there?

Mr. POULOS. Well, we have—we have that bifurcated in terms of corporate IT assets and product security, and there are two different sets of requirements. I can—I don't—can't list them to you off the top of my head, but I can——

Mr. WALKER. Mr. Burt.

Mr. BURT. Congressman, we were fortunate enough to find the gentleman who was the chief information security officer for Health and Human Services at the Federal level, and he's been with us now for a couple of years. So he has vast experience working with various government agencies in that capacity as a chief information security officer.

Mr. WALKER. Let me stay with you, Mr. Burt. I want to unpack this a little bit more. Why is a position like this especially relevant in developing equipment for modern elections?

Mr. BURT. I think as we look forward, it is necessary for someone with deep technical expertise to advise the company in its actions, to do everything it can to make sure that we are making the right decisions to protect the security of our equipment and our services.

Mr. WALKER. Mr. Poulos.

Mr. POULOS. I agree with those comments in terms of a deeper understanding of best practices and where the state of the art is evolving to. It really benefits the security of the products.

Mr. WALKER. Real quickly, for the three of you there, if you were to give yourselves a grade, 1 out of 10, 10 being excellent, the highest mark, as far as your attentiveness to make sure there's no corruption or nothing nefarious, any kind of behavior going on, how would you score your company as far as the time, the attention, the resources that you're putting into this, Mr. Burt?

Mr. BURT. Congressman, we spend a great deal of time on a regular basis. Our effort—I can honestly say our effort is as strong as we are capable of. We are always looking to find ways to improve our effort and to partner with other agencies to improve our ability to mitigate any risks that might be there.

Mr. WALKER. Mr. Poulos.

Mr. POULOS. The security of our products and our infrastructure is a key priority for us. It always has, and it is reflected in not only the amount of time and resources we spend to do it.

Mr. WALKER. Ms. Mathis.

Ms. MATHIS. Same thing. We absolutely dedicate—it's in our DNA. It's pervasive across our people, our process, our procedures, our product.

Mr. WALKER. Thank you very much. And if this doesn't work out, you may have a career in politics since none of you gave me a number answer to the question. So I yield back to my chairwoman.

The CHAIRPERSON. The other gentleman from North Carolina, Mr. Butterfield, is recognized for five minutes.

Mr. BUTTERFIELD. Thank you, Chairperson Lofgren, for convening this very important hearing today. I cannot think of a hearing except for the debate on the War Powers Act that we could be having right now. This is critically important to our democracy, and certainly thank you to the three witnesses for your testimony today.

Mr. Burt, let me start with you, sir, and I want to talk specifically about North Carolina. You know I represent a district in North Carolina. There's been a lot of controversy surrounding your company's recent dealings with elections officials in my State. Some have referred to what transpired as a bait and switch. I don't know if that's warranted or unwarranted. I hope it's unwarranted. Can you please explain to me why you waited so long to tell North Carolina election officials that you did not have enough voting systems to cover the 2020 primaries?

Mr. BURT. Thank you for your question, Congressman. I have read that bait-and-switch comment. The situation in North Carolina, we applied for certification for our system in North Carolina roughly five years ago. We went through all of our testing. The report was written. It went to the State board for approval. And at that point in time, the State board essentially dissolved. There was not a quorum at the state board for over four years.

That system that we got tested five years ago finally got approved this year. Because it was five years old, we immediately went in after that and got our latest and most secure system updated. And it is that system, the most recently certified system, that we've delivered to the citizens of North Carolina. So, if a bait and switch means that we decided to send the most recent and most secure system to the citizens of North Carolina, that is what we did.

Mr. BUTTERFIELD. All right. I'm informed that your company admitted installing remote access software on some of its election systems that it sold over a six-year period. Were any remote wireless-equipped systems sold to elections officials in my State?

Mr. BURT. Congressman, that practice happened between the year 2000 and 2006. No system that we have brought through the

EAC program since the year 2007 has been equipped with any kind of remote access software. We have confirmed that there is no system out there in the country being used today that has a remote access system attached to it.

Mr. BUTTERFIELD. All right. Ms. Mathis, do you support Federal legislation to expand the use of post-election audits like risk-limiting audits in Federal elections?

Ms. MATHIS. We absolutely do.

Mr. BUTTERFIELD. Mr. Poulos.

Mr. POULOS. Absolutely.

Mr. BUTTERFIELD. And Mr. Burt.

Mr. BURT. Yes.

Mr. BUTTERFIELD. Thank you. Do you think that all manual audits of paper records can be conducted on all the voting systems that you currently sell?

Ms. MATHIS. We have a portion of—a subset of our product that actually does not permit risk-limiting audits. There are other audits and other testing that fulfilled a fully ability to confirm the accurate results.

Mr. BUTTERFIELD. All right. Let me ask you, Mr. Poulos. What do you do to ensure that your subcontractors and your manufacturers follow industry best practices on cybersecurity? In other words, do you conduct background checks and the like on your subcontractors?

Mr. POULOS. On our direct subcontractors, yes, we do. And for our manufacturing partners, we make sure that they adhere to ISO standards.

Mr. BUTTERFIELD. Mr. Burt.

Mr. BURT. We do the exact same thing. We perform background checks on the contractors that we hire directly, and any of our manufacturing partners are all ISO certified.

Mr. BUTTERFIELD. This is not a—not a cursory background check? You do an indepth——

Mr. BURT. A criminal—yeah, a detailed background check, and that's part of the ISO certification.

Mr. BUTTERFIELD. And Ms. Mathis, you as well.

Ms. MATHIS. Yes.

Mr. BUTTERFIELD. All right. Are you aware of any cyberattacks in which the attacker gained unauthorized access to your internal systems, corporate data, or consumer data? Ms. Mathis.

Ms. MATHIS. We are not.

Mr. BUTTERFIELD. Do you have any evidence that this has happened?

Ms. MATHIS. We do not, no.

Mr. BUTTERFIELD. All right.

Mr. Poulos.

Mr. POULOS. No, we do not.

Mr. BUTTERFIELD. And Mr. Burt.

Mr. BURT. No, we do not.

Mr. BUTTERFIELD. Thank you. Let's see how I'm doing on time. All right.

Back to you, Mr. Burt. We know you're committed to no longer sell paperless machines, but you are selling the Express Vote with an AutoCast feature that has the voter skip—that has the voter to skip the verification of the paper record. Given that the primary criticism of paperless machines was that they did not have a voter verified paper audit trail, do you think—do you think it's—it's correct to say that you will no longer sell paperless machines, but you are selling a machine that can record votes without a paper trail?

Mr. BURT. Congressman, I don't believe—I'm not aware off the top of my head of any customers who are using that particular product in an AutoCast fashion. I believe all the customers who are using that product present the ballot back to the voter for verification in one way or another, either through a screen or by taking out the piece of paper.

Mr. BUTTERFIELD. All right. And, finally, for Ms. Mathis, currently listed on your website in the products that you sell are the paperless DRA machine called the Verity Touch. I guess I have that right, Verity Touch. Meanwhile, there is a clear consensus among experts that the paper ballots are needed to ensure that voters' votes are counted properly. Why do you think—why do you continue to sell a machine we all know puts the integrity of the voters' ballot at risk?

Ms. MATHIS. We actually believe our DREs are secure, and it's not just Hart's belief. We have had those products federally certified through the EAC. They've gone through extensive accredited test lab testing. Certain States have certified those. They comply with all VVSG standards, and they comply with all our extensive security protocols that we have throughout the Verity—throughout the Verity platform including extensive multilayer defense-in-depth security protocols.

Mr. BUTTERFIELD. Thank you. I'm out of time.

I yield back.

The CHAIRPERSON. The gentleman's time has expired. We'll have a second round of questions so that we can further explore this.

The gentlelady from Ohio is recognized for five minutes.

Ms. FUDGE. Thank you very much.

The CHAIRPERSON. The Chairwoman of our Elections Subcommittee.

Ms. FUDGE. Thank you very much, Madam Chairperson. Thank you all so much for your testimony.

All right. Just a couple of questions, really, but let me just first say I understand that this is a business with you all, but I think my colleague, Mr. Butterfield, said it best: "It is critical to our democracy, and your equipment is purchased with taxpayer dollars." So there are some things that we do expect, and there is some information that we expect you to give us.

So, as I say that, let me just also say that I'm from Cuyahoga County, Ohio. We have ES&S machines, but in the State of Ohio, we have 13 different voting systems. And so, when we talk about ensuring the security of our systems, what we find is that we probably need more trained examiners because we have so many different systems. So let me first ask, do you support increasing the number of testing labs so that we can test voting equipment examiners?

Mr. BURT. Yes, we do.

Ms. FUDGE. Okay.

Mr. POULOS. Absolutely.

Ms. MATHIS. Yes.

Ms. FUDGE. Secondly, it's my understanding that the testing standards that we currently use date back as far as 2005. We're in 2020, but we're using standards. And so what we have done is basically said to the Windows people: You determine what the upgrades in security should be because you're dancing to their tune, not to the EAC.

Is that how you see it as well?

Mr. BURT. Congresswoman, I think there is certainly an opportunity to update the voting systems standards and actually to broaden the program to include more security specific testing. That's what we would like to see.

Ms. FUDGE. Everybody.

Mr. POULOS. I'm sorry, Congresswoman. I don't understand the question.

Ms. FUDGE. Well, you're doing upgrades to your systems on a regular basis, not based upon what we think is a security issue but what Windows is telling you you need to do because that's the operating system.

Mr. POULOS. Both—both is true, actually. So we are regularly innovating new features that are—that come from local jurisdictions and State officials based on evolving threats and evolving state of the art of the technology. In addition, we do use Windows and Microsoft products that do have their own patches. That's not core to the tabulation product as well. We do not have off-the-shelf Windows.

Ms. FUDGE. I'm not suggesting that.

Mr. POULOS. Okay.

Ms. FUDGE. What I'm suggesting is that when you do—when Microsoft calls you and tells you "you need to do this upgrade," you do it.

Mr. POULOS. We implement it. We test it. We submit it for certification. We do not implement it, for example, in a county in Ohio until it is tested.

Ms. FUDGE. I'm not suggesting that you don't test it.

Mr. POULOS. Okay.

Ms. FUDGE. My point is that you don't do it based upon what we believe is a security issue; you do it upon what Microsoft believes is one.

Mr. POULOS. Right. I—okay.

Ms. FUDGE. You don't have to defend Microsoft. I'm not trying to do anything to Microsoft. I'm just making the point that we need to be more involved in the process.

Mr. POULOS. No, that's true. That's true.

Ms. FUDGE. Okay. Will all of you commit today to allowing researchers to test your products without prescreening or hand-picking those researchers to do it?

Mr. BURT. Congresswoman, we're not interested in hand- picking. What we're interested in is making sure that we attract hackers who can make our systems better without requiring that the information that they discover be put into the public domain. So what we'd like to see is for the EAC to actually manage a coordinated vulnerability disclosure program and have the EAC choose the researchers and assemble the team and manage the program. We think that's——

Ms. FUDGE. So that's a yes?

Mr. BURT. Yes. We would like to see the EAC manage that program.

Ms. FUDGE. The only reason I'm cutting you off, I have five minutes.

Mr. BURT. Sure. Understood.

Ms. FUDGE. I ask each of you. What do you do to ensure that your subcontractors and manufacturers follow best practices on cybersecurity? Mr. Butterfield already asked you about your background checks. If you could answer the first part of the question.

Mr. POULOS. Well, in our case, for example, our lead manufacturer manufactures products for the Department of Defense and has accreditations under ISO, and so we look for that as a prerequisite to doing business with that manufacturer.

Ms. MATHIS. Very similar, yes. We look at ISO standards. We also have deep quality reviews and ensure that we're managing our suppliers very, very closely.

Ms. FUDGE. Very good. I work for the Federal Government too. I don't trust everybody else that works for the Federal Government. So I want to be sure that you're looking at them, not just hiring them because they work for the Federal Government.

Mr. POULOS. Fair enough.

Ms. FUDGE. I yield back, Madam Chairperson.

The CHAIRPERSON. The gentlelady yields back.

The gentleman from California, Mr. Aguilar, is recognized for five minutes.

Mr. AGUILAR. Thank you, Madam Chairperson. I wanted to talk a little bit about products and defects, and we can go down the line. Mr. Burt, if you'll indulge me by starting. Do you have built-in systems and practices that look for—specifically look for defects along the way? And can you describe the evolution of how long it takes to find a defect, create a solution, and then implement that solution?

Mr. BURT. We do have built-in systems ranging from various source code reviews to penetration testing to functional testing. In the event—if a system has been fielded, been approved by the EAC and delivered to a State and has been fielded, and there's a—there's a functionality—piece of the functionality that we want to change, that process to make the change currently—have to go through the Federal testing program and redeploy to the State—can be six months to a year depending on the scope and depth of the changes being made.

Mr. AGUILAR. Do you inform the customer when that happens——

Mr. BURT. Yes.

Mr. AGUILAR [continuing]. If a defect or something—are they under an obligation to pay for a fix?

Mr. BURT. No. No. In those cases, those are covered under licenses, and we make the changes and roll them back out to the customer.

Ms. AGUILAR. Mr. Poulos.

Mr. POULOS. Similar with Dominion. We comprehensively do situational testing on all of our products, and that is an ongoing thing in the company on all current products. Any issue that we find is immediately disclosed. That's actually regulated in some States such as your home State within a very specific time period, depending on the severity of the issue.

Mr. AGUILAR. And then, per the license, they would—you would——

Mr. POULOS. It would not be an extra charge, no.

Ms. MATHIS. Very similar. We disclose any of those types of critical election day type malfunctions to the EAC. So that's all—that's all regulated right now.

Mr. AGUILAR. Great. I appreciate it. Shifting gears to—you talked about the Idaho National Lab and some of the DHS testing work that you've done. With respect specifically to cyberattacks, and we all understand the stakes here and what's involved, as do you. Can you talk specifically about how you work with the Federal Government when cyberattacks potentially occur? Do you report those potential intrusions to your customers or to the Federal Government? And do you believe you have an obligation to provide timely notification to customers when a security breach of that product or your company happens? Mr. Burt.

Mr. BURT. We do. We have—we share information with the MS–ISAC and the EI–ISAC. So we don't, for example, share that a specific IP address has been identified as an attempt to penetrate a firewall. Of course, that happens thousands of times a day from all over the world. So that sort of information isn't useful. But through the coordination with DHS and the MS–ISAC, they help us to identify and understand sort of potential attacks that might be exceptionally dangerous.

Mr. AGUILAR. What would that look like? In the last 60 days. How many times would you notify a customer or the——

Mr. BURT. We don't notify customers of the MS–ISAC, but many of the customers participate and receive the same information, so it's sort of—it's not specific to our business. It's commentary about what's going on around the country.

Mr. AGUILAR. So there's no way for a customer to know that there was a potential breach? I'm not talking about a ping at an IP address. I'm talking about a breach and a potential intrusion into your system.

Mr. POULOS. We've had no breaches to report.

Mr. AGUILAR. What's that dialogue like with DHS, with any Federal entity through your systems? How often is that——

Mr. BURT. There is a process if a breach were to occur. DHS has issued guidelines in terms of the communication. We practice those through national tabletop exercises. We actually have the Department of Homeland Security travel to Omaha to conduct a tabletop exercise on premise so that we can essentially practice in the event that a breach did occur to make sure that we would be in position to communicate it effectively.

Mr. AGUILAR. Mr. Poulos.

Mr. POULOS. Very similar, Congressman. We have not had any potential breaches. So we actually haven't reported anything to a customer. But our policy is absolutely that we would immediately communicate any potential breach to a customer.

Mr. AGUILAR. Ms. Mathis.

Ms. MATHIS. Very similar. We have not had any breaches, but we've created a very robust incident response plan that has been updated to include disclosures and notification all directions—DHS, the customer—to ensure that we've got the appropriate communications.

Mr. AGUILAR. At what level would you, Ms. Mathis, would you flag for DHS? I understand that all of you are saying, you know, you haven't been breached.

Ms. MATHIS. Right.

Mr. AGUILAR. But at what level—there's a difference between being breached——

Ms. MATHIS. Right.

Mr. AGUILAR [continuing]. And being pinged by an IP address——

Ms. MATHIS. Right.

Mr. AGUILAR [continuing]. In a foreign country.

Ms. MATHIS. Right.

Mr. AGUILAR. Give me—talk with me about that spectrum of intrusion on the cyber side.

Ms. MATHIS. Right. Well, we actually are erring on the side of, if anything, too much disclosure, if there is such a thing. We actually had an example where a customer contacted us with a potential breach, and we actually contacted the DHS and let them know of this whole situation. So it was not a breach. And, actually, it turned out that that particular county was exercising a test, and so it actually—the whole process worked. We did not know that, and so it was—we were happy to communicate that to DHS.

Mr. AGUILAR. Thank you, Ms. Mathis.

Thank you, Madam Chairperson.

The CHAIRPERSON. The gentleman's time has expired.

As I mentioned earlier, we will have a second round of questions, and I will begin.

In answer to a question from Mr. Butterfield, Mr. Burt testified under oath that they do not currently have voting systems in the United States with remote access software installed, if I heard you correctly.

Mr. BURT. That is our belief, that none of the systems in use today——

The CHAIRPERSON. Would that be true for the other two vendors?

Mr. POULOS. Yes.

Ms. MATHIS. We have never had remote access.

The CHAIRPERSON. Okay. Let me ask you this. Do you sell voting machines that have network capabilities installed?

Mr. BURT. Can you be more specific, Madam Chairperson?

The CHAIRPERSON. Yes. You don't have the software installed, but you have the capability of installing it.

Mr. BURT. For remote access software?

The CHAIRPERSON. Yes.

Mr. BURT. We do not—we no longer install any remote access software. That process was discontinued in 2006 and is not allowed by any of the EAC testing.

The CHAIRPERSON. Mr. Poulos.

Mr. POULOS. Madam Chairperson, we've never had any kind of remote access in our Dominion products.

The CHAIRPERSON. Capabilities.

Mr. POULOS. Capabilities.

The CHAIRPERSON. Okay.

Mr. POULOS. I will say that I do want to draw a caveat. Some of our tabulators have the—are designed around the ability to have an external plug in modem to transmit unofficial results after polls close.

The CHAIRPERSON. Okay.

Ms. Mathis.

Ms. MATHIS. We do not have remote access capabilities, as you mentioned. So, similar to Mr. Poulos, we have, as required by certain States, a remote transmission capability as an add-on.

The CHAIRPERSON. So that's something that we may want to look at further.

I want to talk about remote ballot marking devices. Some experts in election security have raised concerns to me about the risk of these devices that store information about the choice a voter has made in a nontransparent format, for example, a bar code or a QR code, so that when the voter doesn't actually—he may be checking something, but it's not what actually is going to be tabulated. Do you provide that equipment that does it in that way, any of you?

Mr. POULOS. Yes.

Mr. BURT. We do, yes.

Ms. MATHIS. We do not, actually. Our—our technology for our Verity Duo product actually captures—does not put any voter choice in a bar code. We have optical character recognition——

The CHAIRPERSON. Okay.

Ms. MATHIS [continuing]. Technology.

The CHAIRPERSON. I have a question. For over a decade, my smartphone has had the capability to prevent unauthorized, unsigned code from running on the device or interfering with its operating systems. Do all of your election systems currently in use prevent unauthorized code or altering—altered operating systems from running on them in this way?

Mr. BURT. They do, Madam Chairperson. I'll give you one example. The memory stick that we purchased from a U.S. manufacturer, our election management system won't even operate unless they know that it's a particular serialized number memory stick. So, if you bought a memory stick from an Office Depot, it wouldn't recognize, it and the system would shut down.

The CHAIRPERSON. How about you, Mr. Poulos?

Mr. POULOS. Similar. All of our Dominion products that are certified are the same. The exception that I will point out to the Committee is we do support some legacy systems that are still in use that were designed in the remaining cases over 20 years ago that do not have this capability.

Ms. MATHIS. Our Verity product line actually incorporates a feature called white listing which actually only allows the programs that we permit with our Verity design, so it actually blocks everything except for those. So it's the opposite of blacklisting. So it has actually even more secure.

The CHAIRPERSON. I'd like to follow up with you, Mr. Burt, because from the previous testimony, your company is the only one that provides election infrastructure that is not just the voting machines itself. You have indicated your interest or suggestion that the EAC have greater jurisdiction over voter registration, election management systems, electronic poll books, and the like. I'd like to know that even without that jurisdiction, what are you doing right now to ensure that these products are safe, secure, up to date, and utilize current technology best practices?

Mr. BURT. Thank you, Madam Chairperson. With respect to the poll books, all of the data is encrypted on the poll books. With respect to the voter registration systems which I think is more commonly a question for folks, we've recently worked with the Center for Internet Security to install Albert sensors which is a national monitoring system, and we've wrapped this around our voter registration systems that we—that we house.

So, for example, Ranking Member Davis, the example that you brought up related to Illinois going back to the 2016 election, that's the kind of activity that an Albert sensor is meant to detect and prevent with respect to a voter registration system.

The CHAIRPERSON. Thank you very much. I see that my time has expired. So I will turn to the Ranking Member for his additional five minutes.

Mr. DAVIS of Illinois. Thank you, Madam Chairperson.

And thanks again to the witnesses. I think all of our colleagues on both sides of the aisle have the same interest. We want to protect our elections. We want to make sure that all machines that are used to tabulate our free and fair elections are up to the task. So thank you, each of you, for being here today. I know some of the questions can be uncomfortable. I know there's been a lot of talk about supply chain issues. Yes or no questions. We'll start with you this time and go that way, Ms. Mathis. Is it currently possible to build an election machine entirely out of U.S. manufactured parts?

Ms. MATHIS. I don't believe that it is possible today.

Mr. DAVIS of Illinois. Okay.

Mr. Poulos.

Mr. POULOS. Not to my knowledge.

Mr. DAVIS of Illinois. Mr. Burt.

Mr. BURT. I do not believe it's possible.

Mr. DAVIS of Illinois. Do you see why that concerns all of us up here?

Ms. MATHIS. Absolutely.

Mr. BURT. Absolutely.

Mr. DAVIS of Illinois. Are the parts in your supply chain, Ms. Mathis, that come from abroad also used in other industries?

Ms. MATHIS. Yes, they are.

Mr. DAVIS of Illinois. Okay.

Mr. Poulos.

Mr. POULOS. Yes, they are.

Mr. DAVIS of Illinois. Mr. Burt.

Mr. BURT. They are. They're used in a variety. Probably some of them are present in the room today in the various equipment that you see around the room.

Mr. DAVIS of Illinois. Like?

Mr. BURT. We see cameras. We see a variety of electronics. We see switches. There's almost nothing that we interact with from an electronics point of view. Of course, your phone. Thank you. That have parts that are made overseas and distributed to a variety of manufacturers.

Mr. DAVIS of Illinois. So it's the critical components of your election machines that we're all concerned about. And you've testified earlier because we have a global supply chain, you're not able to—you're not able to comprehend a machine that can be built right now with completely U.S. parts. So tell me, tell us, make us feel comfortable here in this country that your machines with the critical components are U.S. manufactured or they're going to be able to not be compromised.

Ms. Mathis.

Ms. MATHIS. I believe that that is an ongoing challenge that we all have, and we're open to getting feedback from—as we mentioned earlier, from DHS to help us understand what our capabilities and opportunities might be to source alternatives.

Mr. DAVIS of Illinois. Mr. Poulos.

Mr. POULOS. That's been an ongoing discussion at the EAC in terms of the next generation of standards on how they address in the guidelines that we would follow to those practices.

Mr. DAVIS of Illinois. Mr. Burt.

Mr. BURT. Again, I think this is an opportunity for the voting system vendors to partner better with the Federal Government. Surely, there is deep talent and expertise in the Federal Government that could be brought to bear on the supply chain management and the voting system industry. We would welcome that dialogue and assistance.

Mr. DAVIS of Illinois. We look forward to working with you in that field.

Earlier, it was mentioned about the campaign contributions and lobbying activities. Mr. Burt, you mentioned that ES&S does not make campaign contributions at the Federal level, right?

Mr. BURT. We actually have a policy that every one of our employees, vice president and above, as well as anyone engaged in sales and marketing activities are strictly prohibited from making district campaign contributions.

Mr. DAVIS of Illinois. Okay.

Mr. Poulos, do you—are you able to make campaign contributions in your company?

Mr. POULOS. We had a policy that all employees were not able to make any campaign contributions.

Mr. DAVIS of Illinois. All right.

Ms. Mathis.

Ms. MATHIS. Similar.

Mr. DAVIS of Illinois. Similar. Are you guys all corporations?

Mr. BURT. Yes.

Mr. POULOS. Yes.

Mr. DAVIS of Illinois. Registered corporations in the United States?

Okay. Well, it's nice to see that we have a lot of agreement here amongst Republicans and Democrats in regard to election security. I find it interesting during the first round of questions Chairperson

Lofgren talked about some of the areas where you all agree that the Federal Government needs to work with you. She mentioned a robust bill sitting in the Senate. Well, here is the problem with the top-down approach from Washington when it comes to our own election infrastructure process. That robust bill sitting in the Senate may force you as corporations to actually give campaign contributions to Members of Congress because, in that robust bill, there's a provision that would take corporate funds from corporate malfeasance which, I would argue, you would be eligible for with election infrastructure if something went wrong, and it would go into a Freedom from Influence Fund that was concocted by the Majority, and that would force the first ever corporate dollars into congressional campaigns. So my point of bringing this up is you don't allow campaign contributions now by any of your employees because you don't want that to affect anyone who's in charge of running free and fair elections in this country, right?

Mr. BURT. Correct.

Ms. MATHIS. Correct.

Mr. POULOS. Correct.

Mr. DAVIS of Illinois. Why in the world would this institution at the Federal level in turn possibly require you and require any corporation to give the first ever corporate dollars to individual Members of Congress' campaigns? That's why, when we talk about robust bills, we all have the same goals, but let's not kid ourselves in thinking that there are provisions in bills that are going to always benefit free and fair elections rather than benefiting individual members of Congress.

I yield back.

The CHAIRPERSON. The gentleman yields back.

I just—before yielding to Mr. Raskin, obviously, everyone's entitled to their own opinion, but the matter referenced is a fine collected by the Federal Government, which would then be put into a fund, not a contribution from corporations.

I yield to the gentleman from Maryland for five minutes.

Mr. RASKIN. Madam Chairperson, thank you very much. Let me pursue the line of questioning by my friend from Illinois, and I asked those questions originally about lobbying and campaign contributions and so on. I just saw this report from ProPublica which says, in August 2018, Louisiana announced it would replace its old voting machines and awarded a $95 million contract to a rival of ES&S which was the lowest bidder. ES&S filed a complaint that accused the State of writing its request for proposals so that only the other companies' machines would satisfy the terms. Shortly after, Governor John Bell Edwards cancelled the deal, effectively siding with ES&S and forcing the State to start the process over again. Quote: "The Governor's administration just sided with the company that was $40 million more expensive," Louisiana Secretary of State Kyle Ardoin said in a statement after the cancellation. In a statement, the Governor's office said the cancellation was justified. The office laid the blame at the feet of the Secretary of State's office, which it said had added additional requirements to the bid just days before responses were due. Louisiana campaign finance records showed that an ES&S lobbyist in Baton Rouge had donated $13,250 to Edwards' campaigns since 2014.

I noted, Mr. Burt, you said that you have a ban on campaign contributions by the top-level officials in your company. Is that right?

Mr. BURT. Correct.

Mr. RASKIN. But it doesn't go all the way down, and it doesn't apply to lobbyists that you would employ in the various States. Is that right?

Mr. BURT. It does not apply to lobbyists, yes.

Mr. RASKIN. So what's your specific practice, Mr. Poulos? None of your employees can make——

Mr. POULOS. Correct.

Mr. RASKIN [continuing]. Contributions at any level? And Ms. Mathis, how about you?

Ms. MATHIS. Correct.

Mr. RASKIN. I wonder if one of you would be interested in opining about why you have that practice and whether you think that should be in Federal law for all of the reasons that were, you know, suggested by my colleague about the importance of keeping election administration completely separate. I mean, you know, we've got two dangers here. One is paranoia where, you know, we have politicians running around saying it's all fraud, right. The other is complacency where we don't pay sufficient attention. But can you explain what the basis of that policy is that you have, Mr. Poulos, for example?

Mr. POULOS. Sure. The basis is very clear. We want as a company and our stakeholders to be completely independent of the election officials that are making selections in terms of what's best for their State and localities. Congressman, in your example of Louisiana, Louisiana happens to be a State that currently has legacy voting systems of the type that is being discussed at this Committee level, and they were seeking to update with more modern certified systems, and, unfortunately, that's been delayed.

Mr. RASKIN. I assume you mean by virtue of the change in the vendor.

Mr. POULOS. There was no change. There was just—because of that process, it was all delayed, and as a result, they're using the legacy voting systems in the 2020 election.

Mr. RASKIN. Gotcha.

Ms. Mathis.

Ms. MATHIS. I'm sorry. What is the question?

Mr. RASKIN. Well, I guess the question is what's the basis of your policy of not—of preventing all employees, and I don't know if it extends to consultants.

Ms. MATHIS. It's just important for to us ensure that we are objective and independent in all elections. We don't run elections. Local election officials run elections, so we're not engaged in the running of the election, but it's just important for us to ensure that we're staying objective and independent.

Mr. RASKIN. I remember that there was a big controversy about the company Diebold, and I think one of your companies took over Diebold. Was that ES&S?

Mr. BURT. A little complicated, Congressman.

Mr. RASKIN. Oh, okay.

Mr. BURT. We made a purchase, and then my colleague, Mr. Poulos here, ended up buying the intellectual property of that.

Mr. RASKIN. Okay. So both of you got a piece of it. But I remember that they were actually politically involved, and I think it was the President who had sent out a campaign solicitation saying that they would do anything to see that one candidate got elected President at a time when their machinery was being used in different States. And that obviously creates a serious problem from the standpoint of public confidence in the integrity of the election.

So all of this makes me think that it might be a good idea for us to formalize and to make comprehensive the practice that you seem to be moving towards which is that your job is to sell the technology, to make it as secure as possible, and not to be involved in the political process.

I'm just wondering, finally, about why it seems that technology goes so wrong sometimes. In Georgia, ES&S owned technology was used where more than 150,000 voters inexplicably did not cast a vote for Lieutenant Governor, and then there were not paper backups. Why does that happen? Because that is one of the problems we have, that there are huge problems like this that take place on the one day or two days a year that the machinery has got work, and then it really undermines public confidence in the whole system.

Mr. BURT. Congressman, the equipment that you speak about is actually not ES&S equipment. The company Diebold that went out of business that you spoke of a second ago——

Mr. RASKIN. Oh, I see. Okay.

Mr. POULOS [continuing]. Is actually the manufacturer of that equipment.

Mr. RASKIN. All right. But in general, I think there were some other cases where that's happened as well. I mean, can you explain? Why does that happen? It only has to work once a year, once every two years, and then it breaks down. So I wonder if maybe one person could answer?

I yield back.

Mr. POULOS. Thank you for the question, Congressman. So the equipment that you are referencing was a legacy voting system originally sold to the State of Georgia by Diebold who is no longer in the elections business. But it is the type of voting machine that does not feature any kind of voter verified paper audit trail. So, in the event of something happening in an election, and that's not the only instance, by the way, where something plausible—or sorry—something possible but not plausible happens, it's difficult to have an audit for that if there's not any kind of paper record.

The CHAIRPERSON. The gentleman's time has expired.

I turn now to the gentleman from North Carolina, Mr. Walker for five minutes.

Mr. WALKER. Thank you, Madam Chairperson. Just a quick purpose of my colleague, Mr. Davis, talking about H.R. 1. A quick question along those lines. I'm assuming if you were fined by the Federal Government, those would be corporate dollars, and you would pay those fines. It makes me think of the great philosopher Yogi Berra who said, "They give you cash, which is just as good as money." We will leave that for a different day.

My question is: We're Federal elected officials. You guys are the experts in this industry, and I applaud you for the in-depth testimonies that you've given today. Obviously, this is not just talking points; you know the stuff here. As I look into the future, and I want all three of you to kind of touch base on this. Where do you see the technology of election systems headed 5, 10, 15, 20 years down the road because, obviously, as the ranking member on another committee when it comes to intelligence and specifically even terroristic cybersecurity acts. So, as technology advances, where do you guys see the adaptations that need to be made over that distance of time? I'm going to start with Ms. Mathis and work right to left today.

Ms. MATHIS. Sure. I mean, unlike other industries in the—other technology industries, the direction seems to be more back to paper. That wasn't the case a few years ago, and now the election industry actually has moved that way to more paper which is interesting from a technology perspective. I feel like that that will continue to evolve as preferences of local election officials evolve and as security continues to evolve. So I think that the answer is it will evolve.

Mr. WALKER. Right.

Mr. Poulos.

Mr. POULOS. I look at it them three ways: in technology, people, and process. On the first, on technology, I see evolved standards on security and how the technology comes to be in terms of manufacturing and supply chain. In terms of people and process, I think that I would like to see, I should say, further programs and continued work at the Federal and State level in terms of better eliminating barriers that jurisdictions have in modernizing their election infrastructure and things like poll worker training.

Mr. WALKER. Okay.

Mr. Burt.

Mr. BURT. I agree with Mr. Poulos' comments on security, and it highlights the fact that the burden on election administrators across the country from a technical capability perspective grows even greater. So I think the challenge for election administrators to be able to staff their respective offices with people who are competent in these fields will be an ever greater challenge going forward.

Mr. WALKER. Thank you very much. I yield the balance of my time to the Ranking Member.

Mr. DAVIS of Illinois. Thank you. And I want to get back to the supply chain issue real quick because it concerns me. Have any of you had conversations with your U.S. suppliers of electronic products that go into your machines just like our TVs, our phones, and what have you? Have you talked to those suppliers you work with that may outsource some of their manufacturing to foreign countries? Have you talked to them about trying to develop a U.S.-made chip or electronic LCD product even though they may be a U.S. company?

Mr. BURT. We have, Ranking Member, but the challenge is—and I believe this is true for all of us. We are not a large customer to any of these major manufacturers, so take Texas Instruments, for example, which makes one of our programmable logic devices. We are a very, very small part of their business. So for them to retool their international operations for our benefit is just not realistic.

Mr. DAVIS of Illinois. Mr. Poulos.

Mr. POULOS. That's a hundred percent correct, and the infrastructure needed is—the change of infrastructure to be able to create all of the fabs and necessary manufacturing for 100 percent components being manufactured in the United States is not a small effort.

Mr. DAVIS of Illinois. Ms. Mathis.

Ms. MATHIS. It will take a whole sea change in the way that the global supply change works in the technology industry, I think, for that—for us to be able to take advantage of that.

Mr. DAVIS of Illinois. Okay. Now, I asked if you were all corporations. Will you tell me, yes or no. Are you—any of you run by private holding companies, private equity companies?

Mr. BURT. We are run by our executive management team, but we have 80 percent ownership by a local private investment group.

Mr. DAVIS of Illinois. How about you?

Mr. POULOS. Similar. We are run by a management team, and we are owned, I believe, 76 percent by a U.S. private equity firm.

Mr. DAVIS of Illinois. All right.

Ms. Mathis.

Ms. MATHIS. Similar structure.

Mr. DAVIS of Illinois. Okay. Do you see why that's concerning to us on both sides of the aisle on election security? That's something that I think—obviously are going to be questions raised by both Republicans and Democrats in the future. Look, I appreciate you all being here. I appreciate you taking the time. We have the exact same interests on all sides here in Washington. We want to protect our elections. We want to make sure your machines are unhackable, and let's continue to work together to make that happen.

I yield back.

The CHAIRPERSON. The gentleman yields back. The gentlelady from California, Mrs. Davis, is recognized for five µminutes.

Mrs. DAVIS of California. Thank you, Madam Chairperson, and thank you to all of you for being here. I'm sorry I had to walk out during the panel for another hearing, but I think many of the questions have been asked.

I wanted to focus for a moment just on voter education and the responsibility, if anyyou all have, you know, through the companies. And also if you want to comment, Ms. Mathis. You know, what is that responsibility? Do you work with election officials? We were talking about some ballots that were misread, you know. How do we deal with that? You mentioned Diebold. That was related—that was related—that was what they did at that particular time, but we also know that sometimes ballots are just not constructed in a way that people actually see where they should go, you know, as they share their stories. So how—you know, what are we doing really to make sure that people are registered correctly, that they can check their votes, make sure that they, you know, voted the way that they want to? Often people are pressured by long lines. How can you help? What are you doing to really address these issues? And I know the second panel is also speaking to voter education.

Ms. MATHIS. We believe very strongly with a partnership with our local election officials, and so that extends to voter outreach, voter training, poll worker training. We work with our local election officials to ensure that they have best practices, that we provide them materials, you know, handouts. We also—we have webinars where we'll train the local election officials toµprovide additional media.

Mrs. DAVIS of California. Can you think of an instance when you've actually picked up a problem, and they've corrected it?

Ms. MATHIS. If they what?

Mrs. DAVIS of California. That you picked up a problem, pointed out something to them that could be an issue and that they changed it.

Ms. MATHIS. Yes. We have the benefit of best practices. We have, you know, customers all over the Nation. We'll provide to them: You know, hey, here is what we've seen in other jurisdictions that's worked really well. So this is an ongoing partnership, and you know, our customers, our local election officials rate us very highly. It's just an ongoing, you know, lifelong partnership with them. We absolutely are part of that solution.

Mr. POULOS. Congressman, what we hear from our customers and what they value is the shared perspective of best practices from our experience around the country with experience that they at that local jurisdiction may not have seen, particularly as it pertains to the deployment of new equipment. Voter outreach and poll worker training is exceedingly important.

We've been asked questions about can we build an un-hackable voting system? And, really, you can have a very secure, reliable, accurate system that's transparent, but again, you have to understand the people and processes layered on top of that and pose additional risks. This is something that voting officials have known for decades. That's why we have poll watchers. It's why warehouses are bipartisan, and boards of election are bipartisan. The poll worker training and the train the trainer is something that is exceedingly important in the ongoing vigilance of the migrating threats that we see.

Mr. BURT. Congresswoman, you mentioned the importance of voter education. We agree. For some, unfortunately, interacting with a piece of technology such as a touch screen or even a voting machine can be somewhat intimidating, and we don't ever want that to be a reason that someone would choose to not go and vote. So starting with making sure that our customers understand at a very deep level how these machines operate and then assisting them, going out in the public. For example, with the city of Philadelphia, we made our machines available in many public squares and invited citizens prior, months in advance of the first election where this equipment would be used so that people could kind of remove the intimidation factor from interacting with a new piece of equipment and make sure that they are comfortable so that they would be encouraged to be able to come out and exercise their right to vote.

Mrs. DAVIS of California. Thank you. I certainly hope we don't hear about some of those horror stories that have occurred from time to time, and it's not all your responsibility, of course, but where you can help I think is helpful.

In the interest of transparency, could you share just this quickly how much of your annual profits, and if you could tell us, you know, what are your annual profits? How much of that money comes from sales of new voting machines, and how much of it comes from service contracts for existing machines?

Mr. BURT. Congresswoman, that varies very substantially from year to year. There are years or there have been years, even recent years where we've sold very minimal amounts of hardware. And, of course, last year in the recent run up in preparation for 2020, I believe all three of our companies sold a disproportionate amount of hardware because of the actions that jurisdictions were taking. But there is no—unfortunately, I wish there were. There is no even or normal in terms of the mix between hardware and services in this industry.

Mrs. DAVIS of California. Annual profits? I think my time is up.

Mr. BURT. Congresswoman, we're a private company, so we'll keep that information private.

Mrs. DAVIS of California. Madam Chairperson, if you want to—does that really represent kind of where you're at as well in terms of——

Mr. POULOS. Correct.

Mrs. DAVIS of California. All right. Thank you. Thank you, Madam Chairperson.

The CHAIRPERSON. The gentleman from North Carolina is recognized for five minutes.

Mr. BUTTERFIELD. Thank you, Madam Chairperson.

Madam Chairperson, the first round went very quickly, and I was unable to ask my final question, and so let me pose it at this time. To all three of you, do your tabulators have wireless modems capacity?

Mr. Burt.

Mr. BURT. We do field some tabulators with wireless modem capability, yes.

Mr. BUTTERFIELD. Do you have any concerns about whether or not that poses any security threats?

Mr. BURT. I think that there's always a concern. That's something that we've discussed with our—with our technology partners and our government partners. We recently assisted with the State of Rhode Island to test a new service where Verizon has a private network that does not travel on the normal internet highway. It's blocked by firewalls on either side. They involved their—their National Guard in these tests and determine that these systems were, in fact, very low risk and that they wanted to continue using them.

Mr. BUTTERFIELD. Does Dominion use wireless modems?

Mr. POULOS. Yes, Congressman. So, in relation to the precinct level machines, we use them insofar as a State has a regulation and requirements to report unofficial results remotely. And the way we do it, so to answer your question on—in terms of a concern, there are additional risks that are posed when you have remote transmission of results. We work to mitigate them with State and local officials. All of our modems have—work on a private network.

Mr. BUTTERFIELD. Ms. Mathis, do you have modems as well?

Ms. MATHIS. Yes. We do similar.

Mr. BUTTERFIELD. I'm going to run out of time this time around. Finally, the Ranking Member raised a few minutes ago our concerns, our bipartisan concerns about private equity. Would you be willing to submit to—each one of you to submit in writing after this hearing a list of all individuals and entities with at least a 50 percent or more—5 percent or more ownership? They said 80 and 76. So I thought I would raise it to 50. Let's say 5 percent or more ownership or controlled interest in your company including private equity.

Mr. POULOS. Congressman, we regularly make that exact disclosure to our customers.

Mr. BUTTERFIELD. But it is 80 percent.

Mr. POULOS. Oh. It's 5 percent, anything over 5 percent. We actually answer all questions to our customers.

Mr. BUTTERFIELD. Didn't you say earlier that 80 percent of your ownership is with——

Mr. POULOS. Ours is—I think it's 76, yeah.

Mr. BUTTERFIELD. Someone said 80 percent? All right. You are not in a position to provide a list of those investors?

Mr. POULOS. Oh, no. We are.

Mr. BUTTERFIELD. All right. All right. it's part of the public record currently.

Mr. POULOS. I don't know if jurisdictions publish it, but we're certainly not adverse to it.

Mr. BUTTERFIELD. If you give it to the customers, then you can certainly give it to this Committee.

Mr. POULOS. Of course.

Mr. BUTTERFIELD. Would you do that?

Mr. POULOS. Of course.

Mr. BURT. Congressman, just to clarify, I believe your question was to disclose anyone who owned 5 percent or more of the business. And my answer is, yes, we will supply that, and we have actually supplied that information to your State of North Carolina.

Mr. BUTTERFIELD. All right.

And Ms. Mathis.

Ms. MATHIS. Yes. Same feedback. So, as far as greater than 5 percent, we have provided that.

Mr. BUTTERFIELD. All right. Thank you. I yield back.

The CHAIRPERSON. The gentleman from North Carolina yields back.

The gentlelady from Ohio is recognized for five minutes.

Ms. FUDGE. Thank you. Again, thank you for being here. I really don't have a question for them. I just have a comment, Madam Chairperson. I'm glad that we agree on the fact that persons who work in your particular companies and in your field should not be making contributions to Members of Congress, but I'm always amused by how we change positions from day to day. One day my colleagues say: Corporations are people, my friend, you know, and they should be able to make contributions.

So I don't know why you shouldn't be able to.

Then they'll say: It's a First Amendment right for people to make contributions.

They oppose campaign finance reform, and then they contort the language of H.R. 1. I'm just always confused about where they stand, so I appreciate your position. I think that it is the correct position, but I don't want you to get crosswise because corporations are people, my friend.

I yield back.

The CHAIRPERSON. The gentlelady yields back.

The gentleman from California is recognized for five minutes.

Mr. AGUILAR. Thank you, Madam Chairperson.

Just one last question to follow up on Mrs. Davis, who asked a little bit about your company's annual profits. And I think it's fair to say that the revenue derived by the companies comes from—would it be fair—let me start there. Would it be fair to say that the revenue that your companies derive comes from those two main sources which is selling machines and then providing services, contracts for services related to those machines and their use. Is that fair?

Mr. POULOS. That's fair.

Mr. BURT. Yes.

Mr. AGUILAR. So, if the three of you control 80 percent of the market, my concern is what portion of your revenue do you invest in research and development to produce better, more secure, more cost-effective machines? Because what I don't want to get to is a position where you three control—we have the same hearing in 2 years, 4 years, and you control 95 percent, and you collectively decide, well we're just going to you know, sell a few machines, provide those contracts to those, and we're going to kind of work with each other to make sure that we don't innovate, you know, continue to grow.

I'm not saying that you folks do. I'm saying that, you know, it wouldn't shock you to say—it wouldn't shock you to hear that folks have come to Congress in the past when their proportionate share of a business gets a little too large, and members have concerns about where that could go.

Mr. Burt, can you talk a little bit about research and development?

Mr. BURT. Sure. I think you raise a very important concern. There are new entrants into our marketplace, however, and some have been quite successful as of late. We've been presented this question before in terms of a percentage of revenue that we reinvest for research and development. Historically, we're somewhere around 19 percent of revenue that gets reinvested as research and development.

Mr. AGUILAR. Mr. Poulos.

Mr. POULOS. Congressman, innovation is critical for us. We are only as good as our—the products that we come out with and certify. Depending on the year because of our revenue fluctuation, it's anywhere from 20 percent as high as 35 percent.

Mr. AGUILAR. Ms. Mathis.

Ms. MATHIS. Yeah. Very similar on our side. Innovation is critical to us, and as far as, you know, the—we are trusted election partners to our local election official customers. So it's imperative to us that we're continuing to innovate and make sure that we're keeping up with or staying ahead of the technology.

Mr. AGUILAR. I didn't hear the percentage or the range.

Ms. MATHIS. We—ours also varies just depending on kind of the year, but——

Mr. AGUILAR. I heard 19 percent. I heard 20 to 35 percent.

Ms. MATHIS. Yes. We're closer to the 25 percent.

Mr. AGUILAR. Okay. Thank you. I appreciate it.

Thank you, Madam Chairperson.

The CHAIRPERSON. The gentleman yields back, and that is all of our questions for moment. However, as I mentioned in my opening statement, we may follow up with written questions after this hearing. If we do that, we do ask that you respond promptly. We thank you very much for your testimony today, and you are excused.

I'd like to call up the next panel, and maybe we can—it's a big panel. We need to put a few more chairs up.

I would like to invite the next panel to take their seats, and I will begin introducing this panel. First, if we can ask the panelists to sit. It's a little crowded, but we've got some great witnesses. First, I would like to introduce Liz Howard. She serves as Counsel for the Brennan Center's Democracy Program. Her work focuses on cyber security in elections. Prior to joining the Brennan Center, Ms. Howard served as Deputy Commissioner for the Virginia Department of Elections. During her tenure, she coordinated many election administration modernization products, including the decertification of all paperless voting systems.

Dr. Matt Blaze is a researcher in the area of secure systems, cryptography, and trust management. He is currently the McDevitt Chair of Computer Science and Law at Georgetown University Law Center. He is a co-founder of the DEFCON Voting Village.

Dr. Juan E Gilbert. Dr. Gilbert is the Banks Preeminence Chair in Human-Centered Computing and Chair of the computer and information science and engineering department at the University of Florida, where he leads the Human Experience Research Lab. He was part of the committee of experts and academics who wrote "Securing the Vote: Protecting American Democracy" for the National Academy of Sciences, Engineering, and Medicine. Dr. Gilbert also created an open-source voting system that is used in Federal, State, and local elections.

The Reverend Dr. T. Anthony Spearman is a member of the Guilford County Board of Elections in North Carolina. He was elected President of the North Carolina NAACP in October 2017. In 2016, Dr. Spearman played an important role in the voter suppression litigation that challenged suppressive voter ID requirements and other legislation that would suppress votes in communities of color and other represented communities.

Commissioner Donald Palmer was confirmed to the EAC in 2019. He is a former Bipartisan Policy Center fellow where he provided testimony to State legislatures on election administration and voting reforms concerning election modernization. Commissioner Palmer was appointed secretary of the Virginia Board of Elections by former Virginia Governor Bob McDonald in 2011, and he served as the Commonwealth's chief election officer until 2014. He formerly served as the Florida Department of State's director of elections, and prior to his work in election administration, he served as a trial attorney with the Voting Rights Section of the Department of Justice's Civil Rights Division. He was a U.S. Navy intelligence officer and Judge Advocate General and was awarded the Navy Meritorious Service Medal and the Navy Commendation Medal and the Joint Service Commendation Medal.

Finally, I'm going to turn to our Ranking Member, Mr. Davis, to introduce Mr. Gianasi.

Mr. DAVIS of Illinois. Thank you, Madam Chairperson.

And, Mr. Palmer, thank you for your service in the JAG Corps. I'd be remiss if I didn't mention Cole Felder, who is sitting behind me, our General Counsel on this Committee, will be leaving to join the JAG Corps just next week, so this will be his last hearing.

So, Cole, thank you for what you've done here. Thank you for your service-to-be for our country.

I'm really proud to announce our last witness, my home election official, county clerk and recorder in Christian County, Illinois, Michael Gianasi. Prior to his appointment and election—appointed in 2017 and elected in 2018—he was also in the private sector but was our Supervisor of Assessment, so not necessarily the most fun job in the county courthouse to deal with property tax assessments, but he did a great job. And I want to tell you: Mike's here because I believe his testimony is going to provide an interesting perspective given his experience as a local county official who has actually administered elections.

I've known Mike almost my entire life, probably from playing youth sports together in the same hometown to graduating high school together and working together as he was a fixture at the courthouse when I was working back in Illinois. Mike and I are good friends. Mike's a Democrat and I'm a Republican. I know that a guy like Mike Gianasi, the only thing he cares about when it comes to administering elections in my home county where I vote is to get it fair, make sure everybody has access to vote, and to ensure that there's no problems, especially on election night. Now, I know that's the concern of everyone. I think Mike's going to give a unique perspective even coming from a small rural county about how something that may be a good idea here in Washington, how it may impact their ability to actually run that election as efficiently and as effectively as possible. This is Mike's first trip to D.C. too. I got to take him on a nice tour of the Capitol last night.

So, Mike, that you enjoy the rest of your trip. I just want to thank you for your opening testimony, and I really want to thank you for your insight that you're going to be able to give to this Committee, to this city, and to this country about what it takes to run an election in places like central Illinois.

And, with that, thanks again for coming, Buddy.

I yield back.

The CHAIRPERSON. Thank you very much.

As you heard with the prior panel, each of you will be asked to testify for five minutes, but your full written statement will be made part of the record.

At this point, I'd like to ask each of you to stand and raise your right hand.

[Witnesses sworn.]

The CHAIRPERSON. The record will note that each witness responded in the affirmative.

So we will turn first to you, Ms. Howard, and we will hear from each of the witnesses.

TESTIMONY OF LIZ HOWARD, COUNSEL, BRENNAN CENTER FOR JUSTICE, WASHINGTON, D.C.; MATT BLAZE, PROFESSOR OF LAW, GEORGETOWN UNIVERSITY LAW CENTER, WASHINGTON, D.C.; JUAN GILBERT, ANDREW BANKS FAMILY PREEMINENCE ENDOWED PROFESSOR & CHAIR, UNIVERSITY OF FLORIDA, GAINESVILLE, FLORIDA; REV. T. ANTHONY SPEARMAN, PRESIDENT, NORTH CAROLINA NAACP, GREENSBORO, NORTH CAROLINA; THE HONORABLE DONALD PALMER, COMMISSIONER, ELECTION ASSISTANCE COMMISSION, SILVER SPRING, MARYLAND; AND MIKE GIANASI, COUNTY CLERK AND RECORDER, CHRISTIAN COUNTY OF ILLINOIS, TAYLORVILLE, ILLINOIS.

TESTIMONY OF LIZ HOWARD

Ms. HOWARD. Thank you. Thank you, Chairperson Lofgren, Ranking Member Davis, and Members of the Committee for holding this hearing and providing me with the opportunity to testify about the ongoing efforts to secure voting systems across the country and the challenges to this progress stemming from a lack of vendor oversight. Today's unprecedented hearing is a much appreciated continuation of this Committee's work to improve the security of our Nation's election infrastructure and an important step towards comprehensive vendor oversight to address the significant security gaps that remain.

Today, I hope to convey three main points: First, election vendors play a critical role in our democracy but have received little or no congressional oversight. Second, despite this lack of oversight, significant progress has been made in improving election security since 2016. Third, there's still more to do to further strengthen our election systems ahead of the 2020 election and beyond. Congress has a critical role to play in that process, including oversight of the vendors that are so important to the security and accuracy of our elections.

The absence of Federal oversight negatively impacts election officials' ability to further strengthen our election infrastructure and is felt most acutely in times of crisis, as I know from my own experience. In 2017, roughly months before a high-profile election, paperless voting machines used across Virginia were publicly hacked at DEFCON, and a password for one of these machines was publicly reported. Even though I was the deputy commissioner of elections, I didn't know if the vendors knew about the vulnerabilities exploited by the hackers, if the vendors had taken any steps to address these vulnerabilities, who owned or controlled the vendors, or if they would promptly and fully respond to any of my questions as they are not—as they were not then and are not now—subject to comprehensive Federal oversight.

In no other subsector designated as critical infrastructure are private vendors allowed to serve critical functions without commonsense oversight. Election officials, voters, and the public deserve answers to questions about our election system vendors.

While the ongoing work of election officials in this Committee has resulted in significant election security progress across the country, these efforts are no substitute for comprehensive oversight of the wide variety of election vendors that play a critical role in the administration of our elections yet are currently subject to little or no Federal oversight or regulation. The comprehensive vendor oversight framework we recommend applies not only to voting system vendors but also to vendors that program and maintain those systems that count and tally votes and build, manage, and maintain voter registration databases and electronic poll books that allow election officials to judge who is eligible to vote.

I was gratified to hear the CEOs of the three leading voting machine vendors embrace these recommendations for comprehensive reform earlier today. We hope that Congress can move quickly to adopt these reforms but understand that it may take a while to fully implement them. In my written testimony, I outline the steps that we recommend Congress take in the short term, which include oversight of the $425 million recently allocated for election security, paying particular attention to if the money is being spent on building robust resiliency plans to detect and recover from successful breaches to ensure that, regardless of whether there is a successful attack, voters will still be able to vote and have their vote counted accurately. In addition, I included steps that Congress should take to protect our election infrastructure after 2020, which include expansion of the EAC's oversight role to include more robust monitoring and disclosure of the security practices and ownership of election system vendors.

While the lack of vendor oversight is a significant concern, and this Committee and election officials across the country have much work to do before and after the 2020 election, it's important to acknowledge the progress made in strengthening our election infrastructure, including our voting systems, since 2016. For example, almost half of the States using paperless voting machines in 2016 have transitioned to now using paper-based voting systems. Congress has allocated almost—a little bit over, actually—$800 million to bolster election security in the States. Awareness of the risk to our election infrastructure has increased dramatically, and election officials across the country are implementing a variety of measures to make our voting systems more resilient and secure.

Thank you for your time. I look forward to your questions.

[The statement of Ms. Howard follows:]

BRENNAN
CENTER
FOR JUSTICE

Committee on Administration
United States House of Representatives

Statement of Elizabeth L. Howard
Counsel, Democracy Program
Brennan Center for Justice at NYU School of Law
January 9, 2020

"2020 Election Security – Perspectives from Voting System Vendors and Experts"

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 discuss our analysis of the important efforts to secure voting systems 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. Given the important role that election vendors play in our nation's election security, this hearing is extremely important. This committee's ongoing oversight efforts have positively impacted the security of our election infrastructure, and Congress has more work to do.

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, including our voting systems, to withstand attack.

I hope to convey three points in my testimony today:

(1) Election vendors play a critical role in our democracy but have received little federal or congressional oversight;

(2) Despite this lack of oversight, there has been significant progress in improving election security in the past few years – particularly since 2016 – as there has been a greater national focus on the issue; and

(3) There is still more to do to further strengthen our election systems ahead of the 2020 election and beyond. Congress has a critical role to play in that process, including oversight of the vendors that are so important to the security and accuracy of our elections.

I. Election Vendors Play a Critical Role in our Democracy, But Federal Oversight is Lacking

In our current federal election system, private companies perform an extensive array of activities for local election jurisdictions. These election vendors design and manufacture voting machines; build and maintain election websites that help voters determine how to register and where they can vote; print and design ballots; program voting machines before each election; and build and maintain voter registration databases, voting machines, electronic pollbooks used to check in voters at the polls, election night reporting software, and more. 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.

More than 80 percent of voting machines in use today are under the purview of the three private election vendors who are testifying before this committee today.[1] A successful cyberattack against any of these companies could have devastating consequences for elections in vast swaths of the country. But it's not just about voting machines. As described above, beyond voting machines themselves, other technologies that play critical roles in our current election system, like voter registration databases and electronic pollbooks, are also supplied and serviced by these and other private companies.

As outlined in our May 2019 testimony before this committee, the threat of hacking, disruption, or manipulation of our election system is very real.[2] Since 2016, national security and intelligence officials have repeatedly sounded the alarm. In November 2019, the Departments of Defense, Homeland Security, and Justice, together with the Director of National Intelligence, Federal Bureau of Investigation, National Security Agency, and Cybersecurity and Infrastructure Security Agency, issued a joint statement warning, "Russia, China, Iran, and other foreign malicious actors all will seek to interfere in the voting process" in 2020.[3] This comes despite

[1] Kim Zetter, "The Crisis of Election Security," *New York Times Magazine*, Sept. 26, 2018, https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html.

[2] Election Security Hearing, Before the Comm. on House Administration, 116th Cong. (2019) (statement of Lawrence Norden).

[3] "Joint Statement from the Department of Justice, DOD, DHS, DNI, FBI, NSA and CISA on Ensuring Security of 2020 Elections," Justice News, U.S Department of Justice, Nov. 5, 2019, https://www.justice.gov/opa/pr/joint-statement-department-justice-dod-dhs-dni-fbi-nsa-and-cisa-ensuring-security-2020.

these agencies' "[increased] level of support to state and local election officials in their efforts to protect elections."[4]

While the threat to our election infrastructure is real, as a bipartisan 2018 U.S. Senate Intelligence Committee report observed, "State local, territorial, tribal, and federal government authorities have very little insight into the cyber security practices of [election] vendors."[5] As the Brennan Center has outlined in a recent report, "A Framework for Election Vendor Oversight," (Appendix A) election vendors are subject to virtually no oversight or transparency requirements by the federal government. As a result, local election officials are left in the dark about the vendors they must work with as they seek to defend American elections from attack.

Election officials are purchasing products, including voting machines, and entering into maintenance and service contracts with these vendors, without even knowing, for example, who are the employees or contractors programming the voting machines? Who is writing any software upgrades? Have they been background checked to see if they are vulnerable to bribery and coercion? Have they received basic training on how to avoid spear-phishing attacks, or not to use public WiFi when transmitting potentially sensitive information? Similarly, election officials have no insight into where these private election vendor employees do their work – are they even located in the United States, or are they engineering machine components while under the jurisdiction of a foreign adversary?

These risks and unanswered questions are not tolerated in other key sectors that impact our national security. Defense contractors, for example, must comply with myriad rules from the handling of classified information to the security of their supply chains.[6] The nuclear power industry is subject to an extensive set of rules governing the fitness and reliability of their personnel.[7] Even colored pencils are subject to more federal regulation than voting systems.[8] To be sure, more than 8,000 state and local election jurisdictions retain primacy in running elections. But only the federal government has the resources to ensure that these local officials have access

[4] "Joint Statement from the Department of Justice, DOD, DHS, DNI, FBI, NSA and CISA on Ensuring Security of 2020 Elections," DOJ.

[5] *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.

[6] See, e.g., *National Industrial Security Program, Operation Manual*, U.S Department of Defense, Feb. 2006, §§ 2-200–2-211, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf.

[7] See generally, 10 C.F.R. §§ 26.1–26.825.

[8] Compare, for example, The Labeling of Hazardous Art Materials Act, 15 U.S.C. 1277, and 16 C.F.R. §§ 1500.14, with 11 CFR §§ 9405.1 et seq. Indeed, Chapter II of Title 11 of the Code of Federal Regulations, the principal regulations applicable to the EAC, does not address the certification of voting systems or any potential oversight of election vendors more broadly. Nor does the legislation that established the EAC (the Help America Vote Act of 2002) — which sets some requirements for voting systems used in federal elections, see 52 U.S.C. § 21081 — require the EAC to issue any mandatory regulations on those topics. See, e.g., 52 U.S.C § 20971 (regarding the certification and testing of voting systems), § 20929 ("The Commission shall not have any authority to issue any rule, promulgate any regulation, or take any other action which imposes any requirement on any State or unit of local government . . ."), § 21101 (regarding the EAC's adoption of voluntary guidance).

to the information and expertise they need to effectively ensure that election vendors' security practices are not endangering federal elections.

As discussed in our recent paper, there are at least five areas where private election vendor practices deserve greater scrutiny and oversight. The first involves reporting and response to breaches or hacks. It has now been widely reported that Russian actors targeted an election vendor in the lead-up to the 2016 election, as Special Counsel Robert Mueller's report to the attorney general and his indictment of 12 Russian intelligence officers also alleged.[9] But despite recent reporting, the public has more questions than answers about this incident. In fact, the public is not even completely certain of the identity of the election vendor involved, much less when the vendor learned of the attacks, what measures to protect against such an attack were in place, and what steps were taken after discovery of the attack, including whether customers were informed, and if so, how promptly. The private company VR Systems has agreed that it appears to be the subject of this allegation, but has denied that it was in fact hacked.[10] Our uncertainty about the basic facts is instructive: We know very little about the incident because we know very little about the security practices of the vendors that supply voting systems and other election infrastructure in general.

There are no federal laws or regulations requiring private vendors to take any action in the event of a cyberattack, or, second, to even attest that they follow good security practices. Voting machines are subject to voluntary federal certification, but the vendors who supply, maintain, and often program those machines, along with integrated products such as electronic pollbooks, are not.[11] Thus, in 2017, ES&S, the country's leading voting system vendor, left the sensitive personal information of 1.8 million Chicago voters publicly exposed on an Amazon cloud server.[12] That information reportedly included "addresses, birth dates and partial Social Security numbers,"[13] information valuable to hackers. Although ES&S sells federally certified voting systems, that certification process does not speak to vendor practices more generally that can affect the security of voters' personal information.

[9] United States v. Netyksho et al., No. 1:18CR00215, 2018 WL 3407381, 26 (D.D.C. Jul. 13, 2018); Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, U.S. Department of Justice, 2019, 50, https://www.justice.gov/storage/report.pdf.

[10] Mueller, *Report on the Investigation into Russian Interference*, 51; Kim Zetter, "Florida Election Vendor Says It Has Proof It Wasn't Breached by Russians," *Politico*, May 23, 2019, https://www.politico.com/story/2019/05/23/florida-vendor-russia-1469086.

[11] A variety of bills, including the Election Security Assistance Act proposed by Rep. Rodney Davis (R–IL) and the Democratic-sponsored SAFE Act and For the People Act, have called for electronic pollbooks, which are not currently considered voting systems and covered by the program, to be included in its hardware and software testing regime." For the People Act, H.R. 1, 116th Cong. (2019), § 3302; Securing America's Federal Elections Act, H.R. 2722, 116th Cong. (2019), § 204; Election Security Assistance Act, H.R. 3412, 116th Cong. (2019), § 3(a).

[12] Dan O'Sullivan, "The Chicago Way: An Electronic Voting Firm Exposes 1.8M Chicagoans," *Upguard*, Dec. 13, 2018, https://www.upguard.com/breaches/cloud-leak-chicago-voters.

[13] Frank Bajak, "US Election Integrity Depends on Security-Challenged Firms," *Associated Press*, Oct. 29, 2018, https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c.

Third, opaque supply chains further exacerbate the problem. In 2019, an IBM Security Services investigation on behalf of Los Angeles County found that compatibility issues between the county's voter list and an ES&S subsidiary's software contributed to nearly 120,000 voters being left out of printed pollbooks and forced to request provisional ballots.[14] But there is no federal oversight of subsidiaries or contractors who work with election vendors to ensure standards of quality and security are met. The Department of Defense has recently stepped up its enforcement of supply chain integrity and security standards in the defense contracting sphere, in recognition of the risk that supply chains can pose to national security interests.[15] No analogous management of supply chain risk is occurring in the election vendor industry, however, as Congress has not authorized any agency to provide guidelines for these vendors more generally.

Insider attacks are a fourth area in which federal oversight of vendors could play a positive role in election security, as vendors that fail to follow best practices for personnel screening and other safeguards could be exposed to malfeasance from within. If an employee of a major election vendor were vulnerable to bribery or other improper influence, they could severely impact election integrity and public confidence by undertaking malicious acts against their employer.

Finally, the federal government could also improve transparency into vendors' ownership and control structures.[16] Over the last several years, the topic of foreign ownership of election vendors has occasionally made headlines. For instance, in 2018, the FBI informed Maryland officials that a vendor servicing the state, ByteGrid LLC, had been under the control of a Russian oligarch with close ties to President Vladimir Putin.[17] Dominion Voting Systems, the second-largest voting machine vendor in the United States, whose voting machines are used by more than one-third of American voters, has its headquarters in Toronto. But aside from concerns with foreign influence and control, lack of insight into election vendor ownership also prevents the public from scrutinizing potential conflicts of interest. Some unscrupulous officials might award vendor contracts in exchange for gifts or special treatment rather than to those that would best

[14] "Report Blames Software Error for Los Angeles Voting Problem," *Associated Press*, Aug. 1, 2018, https://apnews.com/95b056ab2eab47febaf721a1d285a045; *Independent Investigation of Election System Anomalies in Los Angeles County on June 5, 2018*, IBM Security Services, Aug. 1, 2018, http://file.lacounty.gov/SDSInter/lac/1042885_FINALExecutiveSummaryAugust12018.pdf; See also Board of Supervisors, *Request for Approval: Amendment Number Eight to Agreement Number 76010 with Data Information Management Systems, LLC for Voter Information Management System Maintenance and Support Services*, County of Los Angeles, 2015, https://www.lavote.net/documents/05052015.pdf`(identifying ES&S subsidiary Data Information Management Systems, LLC, as vendor responsible for maintaining and servicing Los Angeles County's voter information management system).

[15] Undersecretary of Defense, *Memorandum Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review*, U.S. Department of Defense, Jan. 21, 2019, https://www.acq.osd.mil/dpap/pdi/cyber/docs/USA000140-19%20TAB%20A%20USD(AS)%20Signed%20Memo.pdf.

[16] The Protect Election Systems from Foreign Control Act, sponsored by former Rep. John Delaney (D-MD), would require vendors to be "solely owned and controlled by a citizen or citizens of the United States" absent a waiver.

[17] Mark Morales, "Maryland Election Contractor Has Ties to Russian Oligarch," *CNN*, Jul. 16, 2018, https://www.cnn.com/2018/07/16/politics/maryland-elections-russia/index.html; Chase Cook and E.B. Furgurson III, "FBI Informs Maryland of Election Software Owned by Russian Firm, No Known Breaches," *Capital Gazette*, Jul. 13, 2018, https://www.capitalgazette.com/news/government/ac-cn-russianelection-0714-story.html.

facilitate free and fair elections. Transparency into ownership and control is required for the public to assess whether officials engaged in procurement and regulation have been improperly influenced.

As we know, election vendors were targeted in 2016 and are likely to be targeted in the future. This hearing represents a continuation of this committee's efforts to bolster election security through oversight of these election vendors. It will be the first congressional hearing at which representatives of the three primary voting systems vendors will appear jointly to publicly answer questions about their ownership, operations and conduct, which impact the security of our democracy. While this hearing is an important step, and other congressional oversight efforts are ongoing,[18] much work remains for Congress to do in 2020 and beyond.

II. Important Progress Has Been Made Since 2016

Despite the lack of rigorous oversight, important progress has been made since 2016 toward a more secure election system infrastructure. In January 2017, the Department of Homeland Security (DHS) designated election infrastructure as "critical infrastructure."[19] This designation has resulted in many substantive partnerships and collaborations, such as the Election Infrastructure Subsector Government Coordinating Council (EIS GCC) and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), which have significantly improved information sharing practices between federal, state and local officials. Separately, the Election Assistance Commission (EAC), now with a quorum, continues its work on the updated Voluntary Voting System Guidelines (VVSG), though progress remains slow.

Most importantly, despite the lack of oversight of voting system vendors, significant progress has been made on replacing antiquated machines, particularly paperless machines, as well as in implementing robust audits after elections take place but before official results are certified. To address critical vulnerabilities in our current voting system infrastructure, cybersecurity and national security experts have long recommended these steps,[20] which will positively impact the voter confidence of tens of millions of voters who will cast ballots in the 2020 election using a variety of different machines. In fact, the Senate Select Committee on Intelligence's recent

[18] See e.g., "Warren, Klobuchar, Wyden, and Pocan Investigate Vulnerabilities and Shortcomings of Election Technology Industry with Ties to Private Equity," Oversight Letters. Elizabeth Warren, Dec. 10, 2019, https://www.warren.senate.gov/oversight/letters/warren-klobuchar-wyden-and-pocan-investigate-vulnerabilities-and-shortcomings-of-election-technology-industry-with-ties-to-private-equity; MD. CODE ANN., Election Law §§ 2-109 (2019) (Maryland law requiring ownership disclosure).

[19] "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, Jan. 6, 2017, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

[20] See e.g., Lawrence Norden, *The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost*, Brennan Center for Justice, 2006, https://www.brennancenter.org/publication/machinery-democracy; Lawrence Norden, Aaron Burstein, Margaret Chen, and Joseph Lorenzo Hall, *Post-Election Audits: Restoring Trust in Elections*, Brennan Center for Justice, 2007, https://www.brennancenter.org/publication/post-election-audits-restoring-trust-elections-executive-summary; *Securing the Vote: Protecting American Democracy*, The National Academies of Sciences, Engineering, and Medicine, 2018, https://www.nap.edu/read/25120/chapter/1.

bipartisan report on the Russian government's attack on America's election infrastructure echoed these recommendations and pointedly noted that there was an *urgent* need to secure the nation's voting systems.[21]

State and local election officials around the country have made important progress in implementing these recommendations since 2016. This progress is largely due to the new and acute awareness of the threat that hostile actors pose to the integrity of our elections, coupled with $380 million that Congress began to provide in 2018 to help states bolster their election security. As a result of substantive improvements, our voting systems are more secure today in much of the country.

A. Replacement of Antiquated and Paperless Voting Equipment

Replacing antiquated voting equipment, particularly paperless machines, is a critical step in strengthening our voting systems. Without a paper record of voters' intentions, malicious and accidental errors in machine-tabulated votes cannot be audited and corrected. I know how important this is and, in my former role as deputy commissioner of elections in Virginia, I coordinated the decertification and successful replacement of all paperless voting machines less than 60 days prior to our 2017 gubernatorial election. Since the Virginia decertification, the National Academies of Sciences Engineers and Medicine,[22] bipartisan Senate Select Committee on Intelligence[23] and other experts have identified replacement of paperless voting systems as a crucial priority in protecting our election system infrastructure.

In good news, the antiquated voting systems, including paperless machines, have been almost entirely replaced in battleground states. Michigan replaced its aging paper-based voting equipment statewide after the 2016 election; Ohio approved $114.5 million to replace aging voting machines ahead of the 2020 presidential election; Georgia and Pennsylvania are finalizing their scheduled 2020 replacement efforts;[24] and significant replacement has occurred at the local level in Florida and is ongoing in North Carolina.[25]

[22] *Securing the Vote, NASED,5.*

[23] *Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts Against Election Infrastructure with Additional Views*, U.S. Senate Select Committee on Intelligence, Jul. 15, 2019, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

[24] Jonathan Lai, "Every Pa. county will have new voting machines — with paper trails — in 2020," *Inquirer*, Jan. 1, 2020, https://www.inquirer.com/politics/pennsylvania/pa-new-voting-machines-for-2020-with-paper-trails-20200101.html; Stephen Fowler, "Georgia Completes Pilot Of New Paper Ballot-Based Voting Machines," *GPB News*, Nov. 6, 2019, https://www.gpbnews.org/post/georgia-completes-pilot-new-paper-ballot-based-voting-machines.

[25] Rachel Looker, "State law on voting machines sticky for counties," *National Association of Counties*, Apr. 26, 2019, https://www.naco.org/articles/state-law-voting-machines-sticky-counties; See e.g., Taft Wireback, "North Carolina County Spends $2M Switching to Paper Ballots," *Government Technology*, Nov. 22, 2019, https://www.govtech.com/security/North-Carolina-County-Spends-2M-Switching-to-Paper-Ballots.html; Red Berky, "New voting machines pass the test in Mecklenburg County," *WCNC*, Nov. 7, 2019,

However, state and local election officials still have much work to do. We estimate that as many as 12 percent of voters (approximately 16 million voters) will vote on paperless equipment in November 2020.[26] This compares to 20 percent of voters (27.5 million) in 2016.[27]

While almost all states and jurisdictions are purchasing new paper-based systems, at least one voting system vendor continues to sell new paperless voting machines. Two Texas counties have spent roughly $2.5 million in the past two years on new paperless machines.[28] Upon learning of the significant security concerns associated with paperless machines – after purchasing them – one Texas election official stated, "Whoever's doing all the research, it seems like we should have been in on it a little sooner. Honestly, it's very disturbing."[29] The truly disturbing issue here is that we can be certain the vendor was well aware of the security concerns, but apparently failed to divulge this information to the election official buyer.

My experience with the decertification of paperless voting machines in Virginia also serves as an example of the crucial role—positive and negative—that vendors could play in assisting local election officials as they seek to make further improvements to election security in 2020.

At the beginning of 2017, paperless voting machines were in use on a patchwork basis in roughly 25% of the commonwealth. Mindful of the critical infrastructure designation made in January of that year,[30] and the increasingly concerning revelations about Russia's efforts to interfere with

https://www.wcnc.com/article/news/politics/elections/new-voting-machines-pass-the-test-in-mecklenburg-county/275-3d1221e9-7d4d-4599-a89a-53cf8b7e7b30; The number of jurisdictions using paperless DREs has shrunk drastically in Florida, from 24 jurisdictions in 2016, to only three by November 2019. These three remaining counties are currently working to replace their paperless systems before the 2020 elections. See Eric Geller, Beatrice Jin, Jordyn Hermani and Michael B. Farrell, "The scramble to secure America's voting machines," *Politico*, Aug. 2, 2019, https://www.politico.com/interactives/2019/election-security-americas-voting-machines/index.html.

[26] At least some voters in the following eight states will cast their ballot on a paperless voting machine: Indiana, Kansas, Kentucky, Louisiana, New Jersey, Mississippi, Texas, and Tennessee.

[27] Andrea Córdova McCadney, Lawrence Norden, and Elizabeth Howard, "Voting Machine Security: Where We Stand 6 Months Before the New Hampshire Primary," *Brennan Center for Justice*, Aug. 13, 2019, https://www.brennancenter.org/our-work/analysis-opinion/voting-machine-security-where-we-stand-few-months-new-hampshire-primary.

[28] "Texas must retire paperless voting systems to prevent hacking," *Houston Chronicle*, Apr. 9, 2019, https://www.houstonchronicle.com/opinion/editorials/article/Texas-must-retire-paperless-voting-systems-to-12816376.php ("In one case, a Texas county that tried to do the right thing was hamstrung by poor state leadership. San Jacinto County recently spent a cool $383,000 on a new paperless voting system because no one in Austin or Washington warned against it."); Greg Gordon, "14 states' voting machines are highly vulnerable. How'd that happen?," *McClatchy Washington Bureau*, Apr. 4, 2019, https://www.mcclatchydc.com/news/nation-world/national/article207851784.html ("Vicki Shelly, the election administrator in San Jacinto County, Tex., north of Houston, said she received no alert from Washington or state officials before the county spent $383,000 on its new paperless touch-screen voting system made by Hart InterCivic.").

[29] Gordon, "14 states' voting machines are highly vulnerable. How'd that happen?".

[30] 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.

elections,[31] multiple paperless jurisdictions voluntarily made plans to transition to paper-based voting systems. Election officials in localities without transition plans, which were generally poor and rural, were aware of the security concerns associated with paperless machines, but a lack of resources prevented them from replacing their equipment.

As pressure mounted on DHS over the summer to notify election officials in the "21 states" that they had publicly stated were targets of Russian hackers but refused to identify, DEFCon, one of the longest running and largest annual underground hacking conferences,[32] hosted its inaugural Voting Machine Hacking Village ("Village") exhibit.[33] The Village offered "white hat" hackers access to various models of voting equipment, procured by the event organizers through a variety of methods, that were in use across the country, including in Virginia.[34]

We had serious – and immediate – concerns when news stories published in early August reported that all of the paperless voting machines at DEFCon had been hacked, many "within minutes," and one article even included a password for paperless machines still in use in multiple Virginia jurisdictions.[35] We immediately partnered with the state IT agency, VITA, to conduct security reviews of the paperless machines used in Virginia as we were now facing a drastically different threat environment than just two years earlier.

Shortly thereafter, on September 7, less than 60 days prior to the General Election, we decertified all paperless voting machines. Despite the less-than-ideal timeframe, the transition was successful in all affected jurisdictions, largely due to the tireless efforts of local election officials.

The voting machine vendors, and their in-state representatives, were not helpful during the lead up to the decertification (one vendor even refused to provide a requested voting machine for testing purposes). However, once the decertification decision was made, the vendors were integral partners in the effort to ensure a smooth transition; they rapidly and successfully deployed new paper-based voting systems across the commonwealth. Vendor cooperation and openness will make all the difference as more local election officials seek to use the $425 million Congress has allocated to improve election security and public confidence in the months ahead.

[31] Mueller, *Report On The Investigation Into Russian Interference* (characterizing the Russian government's interferences as a "sweeping and systematic" effort to undermine faith in our democracy); *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1*, SSCI.

[32] "Frequently asked questions about DEF CON," *Def Con*, https://www.defcon.org/html/links/dc-faq/dc-faq.html.

[33] Matt Blaze, et al., *Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, DEFCON 25 Voting Machine Hacking Village, Sept. 2017, https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf.

[34] Ibid.

[35] Sean Steinberg, "Hackers Eviscerate Election Tech Security…Who's Surprised?" *Who What Why*, Aug. 1, 2017, https://whowhatwhy.org/2017/08/01/hackers-eviscerate-election-tech-security-whos-surprised/.

B. Implementation of Robust Post-Election Audits

Paper-based voting machines improve election security because they create a paper record that voters can verify for accuracy before casting their ballot. Election officials can review these hard copy paper records during an audit after the election. However, these paper records will be of "limited security value"[36] unless they are used to check and confirm aggregate electronic tallies containing the ultimate election night results.

Traditional post-election audits, which generally require manual inspection of paper ballots cast in randomly selected precincts or on randomly selected voting machines, can provide assurance that individual voting machines accurately tabulated votes. Multiple states have employed these audits for over a decade. In 2020, including four new states since 2016,[37] 24 states and the District of Columbia will have voter verifiable paper records for all votes cast and require post-election audits of those paper records before certifying election results.[38] In total, these 24 states and the District of Columbia make up 295 electoral votes. The remaining 26 states, totaling 243 electoral votes, do not currently require post-election audits of all votes prior to certifying election results. However, there is nothing stopping most of these remaining states from conducting these audits if they have the resources and will to do so.

Risk-limiting audits (RLAs) are a comparatively new procedure and offer two important improvements to traditional post-election audits. RLAs use statistical methods and a manual

[36] Norden, *The Machinery of Democracy.*

[37] These four states are Rhode Island, Iowa, Georgia, and Pennsylvania. See 17 R.I. Gen Laws §17-19-37.4 (2017); 2017 Iowa Acts 256; H.B. 316, 2019 Leg., Reg, Sess. (Ga. 2019). Pennsylvania, which requires traditional post-election audits before certification in jurisdictions with paper-based equipment, is expected to have replaced all its remaining paperless equipment by the 2020 elections. See Jonathan Lai, "Every Pa. county will have new voting machines — with paper trails — in 2020," Inquirer, Jan. 1, 2020, https://www.inquirer.com/politics/pennsylvania/pa-new-voting-machines-for-2020-with-paper-trails-20200101.html.

[38] For the purposes of this report, the Brennan Center only counted jurisdictions that (1) mandate post-election audits of (2) voter-verified paper records (3) before the certification of election results. These twenty-four states are Alaska, Arizona, California, Colorado, Connecticut, Georgia, Hawaii, Illinois, Iowa, Massachusetts, Minnesota, Missouri, Montana, Nevada, New Mexico, New York, North Carolina, Ohio, Oregon, Pennsylvania, 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. Post-election audits in Illinois and Iowa are not legally binding on election results, while statutes in California, Colorado, Connecticut, Hawaii, Nevada and Utah offer no guidance on whether audits are binding. Other states, which only require post-election audits for jurisdictions that use paper-based equipment (Kansas, Kentucky, Tennessee and Texas) were not included in the list since they still have some jurisdictions using paperless equipment. New Jersey's post-election statute is dependent on the implementation of new voting systems that produce voter verifiable paper records (which have not yet been purchased); *See* "POST-ELECTION AUDITS," National Conference of State Legislatures, last modified November 25, 2019, accessed Jan 6, 2020, http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx; "State Audit Laws Searchable Database," Verified Voting, accessed July 2, 2019, https://www.verifiedvoting.org/state-audit-laws/; Danielle Root, Liz Kennedy, Michael Sozan, and Jerry Parshall, *Election Security in All 50 States: Defending America's Elections*, Center for American Progress, Feb. 12, 2018, https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/.

review of paper ballots to check the accuracy of reported election outcomes.[39] They are generally more efficient than traditional audits, typically requiring a review of a smaller number of ballots during the audit process. And the statistical modeling used is designed to detect potential inaccuracies in overall election outcomes, as opposed to problems with individual machines. RLAs can provide assurance that the reported winner did, in fact, win the election,[40] instead of a traditional audit, which only assures officials that machines are working correctly. Because of these features, the Brennan Center and many other experts have urged broad adoption of RLAs.

States have embraced RLAs at a rapid rate: Colorado was the first state to implement RLAs in 2017.[41] In the following two years, officials in 15 states began experimenting with the procedure in some fashion.[42]

Currently, Colorado and Rhode Island require RLAs before results are legally certified; Nevada will do the same starting in 2022.[43] (Local election officials in Virginia are also required to use the procedure, but only once every five years and only after certification of election results.)[44] Washington and Ohio allow election officials to select RLAs from a set of post-election audit options; California enacted a similar law last year that will apply for most of 2020.[45]

The Brennan Center has long supported both a complete, nationwide transition to paper ballot voting machines and the implementation of risk-limiting audits to ensure security and confidence in electoral results. While the time for the remaining states to replace their antiquated and paperless voting systems prior to the 2020 election is running down, the recent $425 million provided by Congress just last month to bolster election security may enable additional states to transition in the near future and will enable additional states to, at minimum, experiment with robust, statistically sound post-election audits. As they do so, vendors should be forthright and

[39] Elizabeth Howard, *A Review of Robust Post-Election Audits*, Brennan Center for Justice, 2019, https://www.brennancenter.org/our-work/research-reports/review-robust-post-election-audits.

[40] Assuming the reported winner did, in fact, win the election. If the reported winner did not, in fact, win the election, the RLA will detect there is a potential problem with some pre-determined probability, such as 95 percent. See Jerome Lovato, *Risk-Limiting Audits – Practical Application*, U.S. Election Assistance Commission, Jun. 25, 2018, https://www.eac.gov/assets/1/6/Risk-Limiting_Audits_-_Practical_Application_Jerome_Lovato.pdf; Howard, *A Review of Robust Post-Election Audits*.

[41] Ann Marie Awad, "Colorado Launches First in the Nation Post-Election Audits," *NPR*, Nov. 22, 2017, https://www.npr.org/2017/11/22/566039611/colorado-launches-first-in-the-nation-post-election-audits.

[42] These 15 states are Alabama, California, Georgia, Indiana, Michigan, Missouri, New Jersey, Ohio, Oregon, Pennsylvania, Rhode Island, Texas, Virginia and Washington.

[43] Colo. Rev. Stat. Ann. § 1-7-515; 17 R.I. Gen. Laws Ann. § 17-19-37.4(b); The Nevada law requires the state to pilot RLAs during the 2020 election. S.B. 123, 2019 Leg., Reg. Sess. (Nev. 2019).

[44] Va. Code Ann. § 24.2-671.1.

[45] Wash. Rev. Code Ann. §29A.60.185; *Ohio Election Official Manual*, Ohio Secretary of State, Aug. 1, 2018, https://www.sos.state.oh.us/globalassets/elections/directives/2017/dir2017-10_eom.pdf/; The California law authorizes RLAs starting with the March 3, 2020 primary and automatically sunsets at the end of 2020. See Cal. Elec. Code § 15367.

accurate about the security risks inherent in the voting systems they are selling, which may include paperless auditing functionality, and refrain from selling paperless voting machines altogether.

As the months pass, though, it will be harder to replace systems before voters will cast their vote for president. Our focus must shift to further securing the voting systems in place.

III. Congress Has a Critical Role to Play in What is Required to Secure our Elections in 2020 and Beyond

While state and local election officials can take many important steps to strengthen our infrastructure, without congressional action these efforts will result in a patchwork of voting system vulnerabilities across the country. Only Congress can establish a national regulatory framework for election security to safeguard our election infrastructure and Americans' confidence in our electoral system. While this unprecedented hearing is an important step, Congress has much work to do to further protect our election infrastructure in 2020 and beyond.

A. Congress Should Conduct Meaningful Oversight Over Federal Funding for Election Security in 2020

First, it is critical that Congress provide meaningful direction and oversight over how the $805 million that Congress has allocated over the last two years to bolster state election security is used. Ongoing oversight efforts by this committee and others have had a substantive and positive impact on voting system security across the nation. As the committee continues these efforts throughout 2020, it should pay particular attention to the measures that state and local election officials can implement to make our voting networks more resilient before 2020.

While no voting system is 100% secure, election officials should strive to deploy resilient voting systems. Such systems have the "ability… to withstand a major disruption… and to recover within an acceptable time."[46] Regardless of the type of voting technologies used, election officials can implement several commonsense and affordable measures that will make their voting system more resilient and minimize voting delays or interruptions in the event of a voting system failure due to any reason, including error or intentional attack.[47]

Our recent report, *Preparing for Cyberattacks and Technical Failures: A Guide for Election Officials*,[48] (Appendix B) identifies commonsense steps that state and local election officials can

[46] "What is System Resilience," Dictionary, IGI Global, accessed Jan. 6, 2020, https://www.igi-global.com/dictionary/cyber-threats-to-critical-infrastructure-protection/51260.

[47] Edgardo Cortés, Gowri Ramachandran, Liz Howard, and Lawrence Norden, *Preparing for Cyberattacks and Technical Failures: A Guide for Election Officials*, Brennan Center for Justice, 2019, https://www.brennancenter.org/sites/default/files/2019-12/2019_12_ContingencyPlanning.pdf.

[48] Ibid.

take before an election to minimize voting interruptions or delays on Election Day. Although it is not possible to build a voting system that is 100 percent secure against technology failures and cyberattacks, simple and effective resiliency plans nonetheless ensure that eligible voters are able to exercise their right to vote and have their votes accurately counted. With a "giant turnout" predicted for 2020,[49] using a portion of the federal grants soon to be disbursed to state and local election officials to fund these projects is just commonsense.

These measures may vary based on the type of voting system in use and are outlined in our report.[50] For example, jurisdictions relying primarily on direct recording electronic (DRE) voting machines or ballot marking devices (BMDs) should order sufficient paper ballots—generally 35% of registered voters in November 2020—to ensure voting can continue with minimal delay for 2-3 hours of peak voting if voting machines go down on Election Day.[51] Further, while supplies are very important, properly training poll workers on when and how to use these materials is essential.[52]

For jurisdictions primarily relying on voting systems with paper ballots marked by hand, we recommend that election officials print sufficient ballots for 100% of registered voters, and even more in jurisdictions employing election day registration. Many election officials using paper ballots decide how many ballots to print on the basis of prior or predicted election turnout.[53] This approach can result in ballot shortages or outages and leave jurisdictions unprepared for unexpected voter surges.[54] This happened across the country during the 2018 midterm elections[55] when turnout reached historic levels, and many experts predict record-breaking turnout in 2020.[56]

[49] Alexi McCammond, "The Democrats' 100-year flood," *Axios*, May 22, 2019, https://www.axios.com/2020-presidential-election-turnout-predictions-democrats-143ceed4-cda7-4665-9fc3-911387416119.html (" 'The safest prediction in politics is for a giant turnout in 2020,' said Larry Sabato of the University of Virginia. 'Nobody's going to believe the polls after 2016, and everyone will assume a tight race.' ").

[50] Cortés, et al., *Preparing for Cyberattacks and Technical Failures.*

[51] Ibid.

[52] Ibid.

[53] Ibid.

[54] Ibid.

[55] See e.g "Monroe County receives voting extension after some polling locations run out of ballots," *Fox 59*, Nov. 6, 2018, https://fox59.com/2018/11/06/monroe-county-requests-voting-extension-after-some-polling-locations-run-out-of-ballots/; Erin Roby and Mike Valerio, "4 voting locations in Prince George's Co. run out of paper ballots," *WUSA 9*, Nov. 6, 2018, https://www.wusa9.com/article/news/politics/elections/4-voting-locations-in-prince-georges-co-run-out-of-paper-ballots/65-611861358; "High turnout has Missouri polling places running out of ballots," *FOX 2*, Nov. 6, 2019, https://fox2now.com/2018/11/06/high-turnout-has-missouri-polling-places-running-out-of-ballots/.

[56] Alexi McCammond, "The Democrats' 100-year flood," *Axios*, May 22, 2019, https://www.axios.com/2020-presidential-election-turnout-predictions-democrats-143ceed4-cda7-4665-9fc3-911387416119.html (" 'The safest prediction in politics is for a giant turnout in 2020,' said Larry Sabato of the University of Virginia. 'Nobody's going to believe the polls after 2016, and everyone will assume a tight race.' ").

B. The Federal Government Should Enact Comprehensive Election Security Reform to Protect Elections in 2020 and Beyond, and this should include greater oversight of election system vendors

Next, Congress must enact comprehensive election security reform. This comprehensive reform will require consistent funding for election security, as proposed in bills such as the For the People Act and the SAFE Act.[57] It will also require substantive vendor oversight.

Currently, there are no federal laws or regulations requiring private vendors to take any action in the event of a cyberattack, or even to attest that they follow good security practices.[58] Voting systems are subject to voluntary federal certification, but the vendors who supply, maintain, and often program those machines, along with integrated products such as electronic pollbooks, are not. Thus, although a vendor may sell federally certified voting systems, that certification process does not speak to vendor practices more generally that can affect, for example, the security of voters' personal information.

The Brennan Center recommends that Congress adopt a comprehensive system of election vendor oversight by authorizing the EAC's Technical Guidelines Development Committee (TGDC) to issue best practices for election vendors and certify ongoing compliance with those practices.[59] These best practices should address, among other things, the five areas discussed above: (1) cybersecurity best practices; (2) background checks and other security measures for personnel; (3) transparent ownership; (4) processes for reporting cyber incidents; and (5) supply chain integrity.

The certification program should include election vendors and a broader set of elections systems. We believe that voluntary certification will provide vendors with sufficient incentives to comply with best practices while respecting the historic role of states in overseeing their own elections.

Until Congress is able to act, the EAC could significantly improve election officials' insight into voting system vendors' practices by requiring, through its registration process, that voting system vendors provide key information relevant to the five areas discussed above. Enhancing the registration process will better enable election officials to mitigate risks facing our election infrastructure and provide much needed transparency to the voting equipment sales and

[57] For the People Act, H.R. 1, 116th Cong. (2019), § 298D; Securing America's Federal Elections Act, H.R. 2722, 116th Cong. (2019), § 297D.

[58] The Secure Elections Act, S. 2261, 115th Cong. (2017), which had bipartisan support for much of 2018, would have required vendors to notify the relevant election agencies when suspected cyber-incidents occur; in a similar vein, the Election Vendor Security Act, H.R. 6435, 115th Cong. (2018), requires vendors to "report any known or suspected security incidents involving election systems . . . not later than 10 days after the vendor first knows or suspects that the incident occurred.".

[59] The Election Vendor Security Act, sponsored by Rep. Jamie Raskin (D-MD), proposes that state and local election administrators be banned from using any vendor for federal elections that does not meet some minimum standards. H.R.6435, 115th Cong. (2018).

marketing process. While this would not reach vendors who market election infrastructure such as e-pollbooks, but do not sell voting systems, it would be a significant step in the right direction.

congressional reform and agency action can ensure that in the long and short term, our elections are free, fair and secure.

C. The Federal Government Should Provide Consistent and Reliable Election Security Funding

Finally, 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 recently committed an additional $425 million. But these one-time investments are not enough to address the significant problems facing election systems, nor to provide long-term stability for future elections. Senator Warner, Vice Chair of the Senate Intelligence Committee, observed last week, "additional money is no substitute for a permanent funding mechanism for securing and maintaining elections systems." As the Congressional Task Force on Election Security found and numerous national security and election officials have said, "Election security is national security."[60] There is an ongoing need for federal funding to help protect our election infrastructure from foreign threats.

Because the threats to our elections 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.

[60] See e.g., "Secretary Kirstjen M. Nielsen Remarks to the National Election Security Summit: As Prepared for Delivery," *Homeland Security*, Sept. 10, 2018, https://www.dhs.gov/news/2018/09/10/secretary-kirstjen-m-nielsen-remarks-national-election-security-summit ("[E]lection security is national security."); "Department of Homeland Security and Georgia Secretary of State Respond to Misleading News Reports About Georgia Elections," *Georgia Secretary of State*, Jul. 16, 2019, https://sos.ga.gov/index.php/general/department_of_homeland_security_and_georgia_secretary_of_state_respond_to_misleading_news_reports_about_georgia_elections_; *Congressional Task Force on Election Security*, House Committee on Homeland Security, 2018, https://homeland.house.gov/imo/media/doc/TFESReport.pdf; Stephen Montemayor, "Bid to get Minnesota federal election security money picks up early in session," *Star Tribune*, Jan. 7, 2019, http://www.startribune.com/bid-to-get-minnesota-federal-election-security-money-picks-up-early-in-session/504511722/; Francis X. Taylor, "Firewalling democracy: Federal inaction on a national security priority," *Hill*, Jan. 31, 2018, https://thehill.com/opinion/national-security/371251-firewalling-democracy-federal-inaction-on-a-national-security; Open Hearing on "Cyber-securing the Vote: Ensuring the Integrity of the U.S. Election System," Before the House Comm. on Oversight and Government Reform, 115th Cong. (2018) (statement of Maggie Toulouse Oliver, New Mexico Secretary of State), https://www.nass.org/sites/default/files/7.24.18-HouseOGR-2018Elections-MTO.pdf.

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.[61] 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

Despite the lack of vendor oversight, important progress has been made since 2016 to make our voting system infrastructure more secure. Congress has an important role to play and can take immediate steps to support state and local election officials as they work with vendors to replace, audit, and improve the resiliency of their systems in 2020 and beyond.

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

Appendix A

POLICY REPORT

BRENNAN
CENTER
FOR JUSTICE

A Framework for Election Vendor Oversight

Safeguarding America's Election Systems

By Lawrence Norden, Christopher R. Deluzio,
and Gowri Ramachandran PUBLISHED NOVEMBER 12, 2019

Brennan Center for Justice at New York University School of Law

Table of Contents

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that works to reform, revitalize — and when necessary defend — our country's systems of democracy and justice. The Brennan Center is dedicated to protecting the rule of law and the values of constitutional democracy. We focus on voting rights, campaign finance reform, ending mass incarceration, and preserving our liberties while also maintaining our national security. Part think tank, part advocacy group, part cutting-edge communications hub, we start with rigorous research. We craft innovative policies. And we fight for them — in Congress and the states, in the courts, and in the court of public opinion.

ABOUT THE BRENNAN CENTER'S DEMOCRACY PROGRAM

The Brennan Center's Democracy Program encourages broad citizen participation by promoting voting and campaign finance reform. We work to secure fair courts and to advance a First Amendment jurisprudence that puts the rights of citizens — not special interests — at the center of our democracy. We collaborate with grassroots groups, advocacy organizations, and government officials to eliminate the obstacles to an effective democracy.

STAY CONNECTED TO THE BRENNAN CENTER

Visit our website at **www.brennancenter.org**

Executive Summary

More than 80 percent of voting systems in use today are under the purview of three vendors.[1] A successful cyberattack against any of these companies could have devastating consequences for elections in vast swaths of the country. Other systems that are essential for free and fair elections, such as voter registration databases and electronic pollbooks, are also supplied and serviced by private companies.

Yet these vendors, unlike those in other sectors that the federal government has designated as critical infrastructure, receive little or no federal review. This leaves American elections vulnerable to attack. To address this, the Brennan Center for Justice proposes a new framework for oversight that includes the following:

- **Independent oversight.** A new federal certification program should be empowered to issue standards and enforce vendors' compliance. The Election Assistance Commission (EAC) is the most logical agency to take on the role. Unfortunately, from its founding, the EAC has had a history of controversy and inaction in carrying out its core mission. In this paper, we assume that the EAC would be charged with overseeing the new program, and we make a number of recommendations for strengthening the agency so that it could take on these additional responsibilities. Whichever agency takes on this role must be structured to be independent of partisan political manipulation, fully staffed with leaders who recognize the importance of vendor oversight, and supported by enough competent professionals and experts to do the job.
- **Issuance of vendor best practices.** Congress should reconstitute the EAC's Technical Guidelines Development Committee (TGDC) to include members with more cybersecurity expertise and empower it to issue best practices for election vendors. (The TGDC already recommends technical guidelines for voting systems.) At the very least, these best practices should encourage election vendors to attest that their conduct meets certain standards concerning cybersecurity, personnel, disclosure of ownership and foreign control, incident reporting, and supply chain integrity. Given the EAC's past failures to act on the TGDC's recommendations in a timely manner, we recommend providing a deadline for action. If the EAC does not meet that deadline, the guidelines should automatically go into effect.
- **Vendor certification.** To provide vendors a sufficient incentive to comply with best practices, Congress should expand the EAC's existing voluntary certification and registration power to include election vendors and their various products. This expanded authority would complement, and not replace, the current voluntary federal certification of voting systems, on which ballots are cast and counted. Certification should be administered by the EAC's existing Testing and Certification Division, which would require additional personnel.
- **Ongoing review.** In its expanded oversight role, the EAC should task its Testing and Certification Division with assessing vendors' ongoing compliance with certification standards. The division should continually monitor vendors' quality and configuration management practices, manufacturing and software development processes, and security postures through site visits, penetration testing, and cybersecurity audits performed by certified independent third parties. All certified vendors should be required to report any changes to the information provided during initial certification, as well as any cybersecurity incidents, to the EAC and all other relevant agencies.
- **Enforcement of guidelines.** There must be a clear protocol for addressing violations of federal guidelines by election vendors.

Congressional authorization is needed for some but not all elements of our proposal. The EAC does not currently have the statutory authority to certify most election vendors, including those that sell and service some of the most critical infrastructure, such as voter registration databases, electronic pollbooks, and election night reporting systems. For this reason, Congress must act in order for the EAC or other federal agency to adopt the full set of recommendations in this report.[2] Regardless, the EAC could, without any additional legislation, issue voluntary guidance for election vendors and take many of the steps recommended in this paper as they relate to voting system vendors. Specifically, it is our legal judgment that the EAC may require, through its registration process, that voting system vendors provide key information relevant to cybersecurity best practices, personnel policies, and foreign control. Furthermore, the EAC may deny or suspend registration based on noncompliance with standards and criteria that it publishes.

Ultimately, the best course of action would be for Congress to create a uniform framework for election vendors that adopts each of the elements discussed in this paper. In the short run, however, we urge the EAC to take the steps it can now to more thoroughly assess voting system vendors.

Introduction

The unprecedented attacks on America's elections in 2016, and repeated warnings by the country's intelligence agencies of future foreign interference, have raised the profile of election security in a way few could have imagined just a few years ago. The response has largely focused on improving the testing of voting machines before they are purchased and on training state and local election officials to institute best practices to prevent, detect, and recover from cyberattacks.

Yet private vendors, not election officials, build and maintain much of our election infrastructure. They create election websites that help voters determine how to register and where to vote; print and design ballots; configure voting machines; and build and maintain voter registration databases, voting machines, and electronic pollbooks. Not every jurisdiction outsources all of these functions, but all rely on vendors for some of this work and many for nearly all of it. Understandably, many local governments under fiscal pressure would rather contract out these functions than increase their election office staff, especially considering the cyclical nature of election-related work.

There is almost no federal regulation of the vendors that design and maintain the systems that allow us to determine who can vote, how they vote, or how their votes are counted and reported. While voting systems are subject to some functional requirements under a voluntary federal testing and certification regime, the vendors themselves are largely free from federal oversight.

This is not the case in other sectors that the federal government has designated as critical infrastructure. Vendors in the defense sector, for example, face substantial oversight and must comply with various requirements, including rules governing the handling of classified information and supply chain integrity. The federal government regulates colored pencils, which are subject to mandatory standards promulgated by the Consumer Product Safety Commission, more stringently than it does America's election infrastructure.[3]

There is a growing bipartisan appreciation that federal action is needed to address the risks that vendors might introduce into election infrastructure. Rep. Zoe Lofgren (D-CA), who chairs the Committee on House Administration, has said that a significant election-related "vulnerability comes from election technology vendors . . . who have little financial incentive to prioritize election security and are not subject to regulations requiring them to use cyber security best practices."[4] Alabama's Republican secretary of state, John Merrill, has called for the EAC to undertake "a centralized effort to evaluate the effectiveness of election equipment, whether it be for voter administration purposes, electronic poll books," or the like.[5]

While state and local governments retain primacy in running elections, only the federal government has the resources and constitutional responsibility to ensure that the more than 8,000 local election jurisdictions have access to information and expertise to safeguard federal elections from insecure vendor practices.[6] The ability of a foreign power to exploit the vulnerabilities of a vendor in a single county in Pennsylvania could have extraordinary repercussions for the country.

Given the lack of federal oversight, the relatively small number of vendors with significant market share,[7] and

Vendor Involvement in Elections

>> Voter Registration Database
Voter registration information is housed in statewide databases that in many jurisdictions are created or maintained by a vendor.

>> Ballot Programming
Prior to every election, voting machines must be programmed with a memory card or USB stick to display the ballot or read and count votes. Vendors often provide the software.

>> Electronic Pollbooks
On Election Day, poll workers in most jurisdictions check voters in using electronic pollbooks, which are usually provided by a vendor.

>> Voting Systems
Jurisdictions use a variety of voting machines, all provided by vendors.

>> Election Night Reporting
On election night, the general public can view election results through reporting websites that are often provided by vendors.

>> Postelection Audits
After an election, vendors and their equipment play a role in checking that the equipment and procedures used to count votes worked properly and that the election yielded the correct results.

their "severe underinvestment in cybersecurity,"[8] the Brennan Center proposes that the federal government take on a more substantial oversight role. Under our proposal, the EAC would extend its existing certification regime from voting systems to include all vendors that manufacture or service key parts of the nation's election infrastructure. The commission would also continuously monitor vendors, with the power to revoke certification. (The EAC currently has that power but only uses it to oversee the systems themselves.)

Definition of Election Vendor

This paper refers to "election vendors" when discussing those entities that provide election services to jurisdictions throughout the United States. A 2017 University of Pennsylvania report on the election technology industry described these entities as those "that design, manufacture, integrate, and support voting machines and the associated technological infrastructure."[9] While the report focused largely on voting systems, quantifying the sector's annual revenue at $300 million,[10] the election vendors referred to also include those that do not participate in the voting systems market but provide other election-related goods and services. For the purposes of this paper, "vendor" is defined to include any private individual or business that manufactures, sells, programs, or maintains machines that assist in the casting or tallying of votes, voter registration databases, electronic pollbooks, or election night reporting systems.

Vendors Present Points of Attack into Election Infrastructure

Private vendors' central role in American elections makes them prime targets for adversaries. Yet it is impossible to assess the precise level of risk associated with vendors — or how that risk impacts election security. As a 2018 U.S. Senate Intelligence Committee report observed, "State local, territorial, tribal, and federal government authorities have very little insight into the cyber security practices of [election] vendors."[11]

This limited visibility into vendors includes

- vendor cybersecurity practices (how vendors protect their own information technology infrastructure and data);
- foreign ownership of vendors (whether foreign nationals, or agents of foreign governments, own companies performing critical election functions);
- personnel policies and procedures (whether background checks and other procedures are in place to safeguard against inside attacks);
- cybersecurity incident response (how vendors alert relevant authorities of attacks); and
- supply chains (where parts, software patches, and installations come from; how are they transported; and how they are kept secure).

Revelations that Russian actors targeted an election vendor in the lead-up to the 2016 election provide a useful example of how little insight there is into vendor security.

Special Counsel Robert Mueller's report to the attorney general and indictment of 12 Russian intelligence officers both included allegations that these officers hacked a private U.S. elections systems vendor. The vendor is believed to operate in at least eight states, including the battleground states of North Carolina, Virginia, and Florida.[12]

According to the special counsel, hackers gained access to the vendor's computers and used an email account designed to look like the vendor's to send spearphishing emails to Florida election officials.[13] Per the indictment, "the spearphishing emails contained malware that the Conspirators embedded into Word documents bearing [the vendor's] logo."[14] According to Florida Governor Ron DeSantis, the hackers breached the election systems of two Florida counties.[15]

We still don't know all the facts. Even in the rare instance that the public learns of a vendor hack — as it did through the special counsel's investigation — many questions remain unanswered. When and how did the vendor learn of these attacks? What preventive measures were in place? What steps did the vendor take after discovering it was targeted to ensure that it was not infiltrated? Did it immediately inform its customers? The public generally never learns the answers to these questions, and there are no federal laws or regulations requiring private vendors to take any action in the event of a cyberattack.

Similarly, *Vice* recently reported that election night reporting systems sold by Election Systems and Software (ES&S), the country's leading election vendor, had been exposed to the public internet, potentially for years on end. (ES&S denied the substance and significance of the report.) Although ES&S voting machines are certified by the EAC, its transmission configuration is not.[16]

The lack of visibility into vendors and their cybersecurity can also contribute to an inability to detect poor practices that might affect vendor performance until it is too late. In 2017, ES&S left the sensitive personal information of 1.8 million Chicago voters publicly exposed on an Amazon cloud server.[17] That information reportedly included "addresses, birth dates and partial Social Security numbers,"[18] information valuable to hackers.

Opaque supply chains further exacerbate the problem. Earlier this year, an IBM Security Services investigation on behalf of Los Angeles County found that compatibility issues between the voter list and an ES&S subsidiary's software contributed to nearly 120,000 voters being left out of printed pollbooks and forced to request provisional ballots.[19]

Although the EAC can conduct manufacturing site visits through its Quality Monitoring Program,[20] this program extends only to voting systems that are submitted for voluntary certification and does not cover the full menu of vendor products and services. There is no federal scrutiny of supply chains for components sourced for noncertified products and services, for example, despite the finding of the Department of Homeland Security (DHS) that "contractors, sub-contractors, and suppliers at all tiers of the supply chain are under constant attack."[21]

The recent ban on certain technologies made by the Chinese company Huawei is a stark illustration of the growing recognition of supply chain risk.[22] Vendors' use of local or regional partners or subcontractors adds to the lack of visibility. For instance, Unisyn Voting Solution, a digital scan voting system manufacturer whose systems have been certified by the EAC, identifies a range of partners in several states on its website.[23] Neither Unisyn nor these partners are currently subject to the kind of oversight we recommend.

> The ability of a foreign power to exploit the vulnerabilities of a vendor in **a single county in Pennsylvania** could have extraordinary repercussions.

Election officials often depend on vendors whose practices are opaque. Yet these companies — unlike those in other critical infrastructure sectors, such as defense, nuclear, dams, and energy — face almost no federal oversight of their security systems. There are no requirements that vendors report breaches, screen employees' backgrounds, patch security flaws, report foreign ownership or control, or ensure the physical security of sensitive software and hardware.

Independent Federal Oversight

This paper assumes that the Election Assistance Commission would be the agency charged with overseeing election vendors. There are many reasons why the EAC is the most logical choice for this role. One among them is that the EAC already certifies voting equipment and issues voluntary guidance. Because it is structured as an independent agency with bipartisan membership, it faces less risk of undue political meddling in the technical work of overseeing election vendors than a traditional executive agency would. Its structure could also help avoid dramatic shifts in oversight approaches with a change of presidential administrations.[24]

Unfortunately, the EAC has been plagued by controversy for years. Its leaders have waded into contentious issues, such as voter identification and proof of citizenship, that have little relation to the agency's core responsibilities.[25] It has missed deadlines for completing critical functions, such as adopting voting system guidelines.[26] And there are concerns that it has not taken election security seriously enough,[27] as well as "complaints of infighting, high [staff] turnover and cratering morale."[28]

If the EAC were chosen for this role, Congress would need to take a number of actions to make its success more likely. First, it would need to increase the agency's budget. The new role would constitute a major expansion of the EAC's regulatory mandate. In recent years, despite the increased threat of cyberattacks against our nation's election infrastructure, funding for the EAC has dropped sharply. The agency's budget in fiscal year 2019 was just $9.2 million, down from $18 million in fiscal year 2010.[29]

With expanded oversight authority, the EAC would need to dramatically increase its cybersecurity competency and knowledge. To facilitate this increased technical focus, we outline below how the existing Technical Guidelines Development Committee would need to be modified to emphasize technical proficiency and, specifically, cybersecurity expertise. We also recommend greater deference to this modified technical committee, permitting its recommended voluntary guidelines to take effect absent overriding action by the EAC. These changes, too, would require congressional action.

On the personnel front, Congress would need to commit to keeping EAC seats filled by leaders who are dedicated to working with each other and with career staff to ensure the security of our election infrastructure. Congress's failure to replace commissioners left the EAC without a quorum between December 2010 and December 2014 and then again between March 2018 and February 2019.

Finally, given the breadth and scope of this new mandate, Congress would need to subject the agency to more scrutiny and oversight than it has in the past.[30]

If Congress is unable or unwilling to take these steps, it should find a different agency to oversee election vendor certification. Any agency placed in that role must be structured so as to remain independent of partisan control. It will need experienced, effective staff and leadership who are committed to election security, cybersecurity, technical competency, and good and effective election administration.

How to Expand Voting System Vendor Registration without Legislation

Most of the policies suggested in this report will require congressional authorization. Not least of these is the ability of the Election Assistance Commission's regulatory authority to reach election system vendors for products and services other than voting machines — including voter registration databases, electronic pollbooks and election night reporting. However, the EAC can under its current authority institute a voluntary system of oversight of the security practices of vendors that supply voting systems, using a combination of its registration and certification schemes.

In order to register, voting system vendors must already provide the EAC with critical information about their ownership, along with written policies regarding their quality assurance mechanisms. Vendors must agree to certain program requirements, and registrants can be suspended if they fail to continue to abide by the registration requirements. A system cannot be submitted for certification unless its manufacturer is currently registered with the EAC.[i] The need for this type of information is clear: in order to carry out its certification, decertification, and recertification authority, including the provision of a fair process to vendors who risk decertification or denial of certification, the EAC must be able to maintain communication with voting system vendors and ensure compliance with quality assurance mechanisms on an ongoing basis.

To ensure that certified voting systems are secure, the EAC can adopt Voluntary Voting System Guidelines (VVSG) that outline best practices for vendors as they relate to cybersecurity, personnel, foreign control, and supply chain integrity. Voting system vendors can then be required, as part of registration, to provide information on their compliance with these standards.

For instance, the current VVSG provide special guidelines for voting systems that use public telecommunications networks in order to ensure that they are protected against external threats, including monitoring requirements. Similarly, the guidelines require verification methods for both software setup and any software update packages.[ii] New guidelines could outline why background checks for personnel are necessary to ensure the ongoing security of voting systems, including upgrades and changes.[iii]

The current registration process could also allow the EAC to ensure that various voting system vendor best practices remain in force over time. The process imposes a continuing responsibility on vendors to report any changes in the information supplied to the EAC and to "operate . . . consistent with the procedural requirements" established by the EAC's testing and certification manual. Thus, if registration mandated, for example, the provision of cybersecurity information from vendors, they would be required to report cybersecurity changes or incidents pursuant to their responsibility to keep registration information up to date. Registration could be suspended if vendors failed to maintain policies consistent with the EAC's requirements.[iv]

While expanding oversight of voting system vendors to ensure compliance with the basic security measures discussed in this paper would not be a substitute for a full certification system for all election system vendors, it would be a significant step toward providing greater accountability for voting system vendors.

A New Framework for Election Vendor Oversight

Under the Brennan Center's proposal, the Election Assistance Commission's oversight role would be substantially expanded. Oversight would extend beyond voting equipment[31] to election vendors themselves. The current voting system testing is intentionally quite limited: it occurs at the end of the design, development, and manufacture of voting system equipment. It does not ensure that the vendors have engaged in best supply chain or cybersecurity practices when developing equipment or when servicing or programming it once it is certified.[32] Nor does the system ensure that the vendor has conducted background checks on employees or set up controls limiting access to sensitive information.

Despite its limitations, the EAC's Testing and Certification Program — a voluntary program that certifies and decertifies voting system hardware and software — provides a good template for a vendor oversight program. A variety of bills, including the Election Security Assistance Act proposed by Rep. Rodney Davis (R–IL) and the Democratic-sponsored SAFE Act and For the People Act, have called for electronic pollbooks, which are not currently considered voting systems and covered by the program, to be included in its hardware and software testing regime.[33]

Currently, the Technical Guidelines Development Committee, a committee of experts appointed jointly by the National Institute of Standards and Technology (NIST) and the EAC, sets certification standards for voting systems. These guidelines, known as the Voluntary Voting System Guidelines (VVSG), can be adopted, with modifications, by a majority of EAC commissioners. Once approved, they become the standards against which voting machines are tested for federal certification. The VVSG ensures that voting systems have the basic functionality, accessibility, and security capabilities required by the Help America Vote Act (HAVA).[34]

Future iterations of the VVSG and certification process may change slightly: commissioners have suggested that they may support a new version of the VVSG that adopts high-level principles and guidelines for the commission to approve, along with a more granular set of certification requirements, which staff could adjust from time to time.[35]

Once new voting system guidelines are adopted, the EAC's Testing and Certification Division tests the systems (per the VVSG), certifies them, monitors them, and, if critical problems are later discovered, decertifies them. The EAC conducts field tests of voting machines only if invited or given permission by a state election official. It does not do this on a routine basis.[36] Rather, election officials using the certified voting machines have the option to report system anomalies to the EAC. If the EAC deems a report credible, it may begin a formal investigation and work with the vendor to address the problem. If the vendor fails to fix the anomaly, the EAC is obligated to decertify the voting system.[37]

With some important modifications, we recommend a similar regime for certifying election system vendors. The commissioners should adopt a set of principles and guidelines for vendors recommended by a Technical Guidelines Development Committee, as well as a more detailed set of requirements that could be adjusted as needed by EAC staff. We recommend that the EAC routinely monitor certified vendors to ensure ongoing compliance and establish a process for addressing violations of federal standards, including through decertification.

A Voluntary Regime

Federal certification will only be meaningful if state and local governments that contract with election system vendors rely on it when making purchasing decisions.

For this reason, some have recommended that state and local governments be required to use only vendors that have been federally certified. For instance, the Election Vendor Security Act proposes that state and local election administrators be banned from using any vendor for federal elections that does not meet some minimum standards.[38]

There are obvious benefits to a mandatory regime. Most important, it would ensure that all jurisdictions throughout the country use vendors that have met minimum security standards. But there are drawbacks as well. Not least of these is that some states and localities might view a federal mandate to use certain vendors as a usurpation of their power to oversee their own elections, making the creation of a federal program politically challenging.

Moreover, since private vendors are so deeply entwined in the running of our elections, requiring towns, counties, and states to use only certified vendors could present problems. If a vendor failed the certification process (or decided not to apply for certification), some counties would not be able to run their elections. Others might be forced to spend tens of millions of dollars to purchase new equipment and services before they could run elections again, even if they had determined that they could have run their elections securely.

A voluntary approach — leaving it to the states and local jurisdictions to decide whether to contract with non–federally certified vendors — could draw states into the voting system certification process. It may also be more politically feasible. A voluntary approach would give state and local jurisdictions the flexibility to take additional security measures if their current vendors did not obtain federal certification. In selecting new vendors, most states and local election officials would likely rely on federal certification in making purchases, as they do with voting machines. Democrats in Congress opted for this approach in the For the People Act and the SAFE Act. Both measures would incentivize participation by providing grants to states that acquire goods and services from qualified election infrastructure vendors or implement other voting system security improvements.[39]

The drawback of a voluntary program is that states and vendors may ignore it. But there is reason to believe that there would be wide participation in a voluntary federal program. Even though the current voting machine certification program is voluntary, 47 of 50 states rely on the EAC's certification process for voting machines in some way.[40] Another voluntary program, DHS's Election Infrastructure Sector Coordinating Council, was founded in 2018 to share information among election system vendors. Numerous major election vendors have supported it as organizing members.[41]

Guidelines Developed by an Empowered, More Technical Committee

A new Technical Guidelines Development Committee, with additional cybersecurity experts, should be charged with crafting vendor certification guidelines for use by the Election Assistance Commission, incorporating best practices that election vendors must meet. These guidelines should go into effect unless the EAC overrides the recommendation within a specified period of time. This deference to the technically expert TGDC in the absence of an override by policymakers is necessary to avoid the kinds of lengthy delays that have stood in the way of prior attempts to update the VVSG.[42] The NIST cybersecurity framework should be the starting point for these best practices, and the TGDC need only apply election-specific refinements to this existing framework.

The TGDC is chaired by the director of the NIST. Its 14 other members are appointed jointly by the director and the EAC.[43] We recommend that Congress authorize NIST to expand TGDC's membership to include the wider range of expertise necessary to fulfill its role in defining vendor best practices. These new members should explicitly be required to have cybersecurity expertise. Congress should also mandate that a representative from the new DHS Cybersecurity and Infrastructure Security Agency (CISA), a leading voice in cybersecurity defense, including in the elections sector, join the TGDC. The Vendor System Cyber Security Act of 2019, introduced by Sen. Gary Peters (D-MI), would require this step.[44] Similarly, Congress should mandate the inclusion of a representative from the National Association of State Chief Information Officers (NACIO) with expertise in cybersecurity.[45]

Reconstituting the TGDC in this manner would not only ensure that it has the relevant expertise to set guidelines for vendors but also that there are more members with technical backgrounds.

As noted above, we recommend permitting the guidelines developed by the TGDC to take effect in the event that the EAC fails to act on them within a specified time period. We also recommend that vendors seeking certification must always meet the most recent set of guidelines. This, along with the expanded membership of the TGDC, will provide the necessary assurance that best practices are updated in a timely fashion and that vendors seeking certification meet the most up-to-date standards.[46]

The new TGDC will be responsible for developing federal certification guidelines that vendors must satisfy to sell key election infrastructure and services for use in federal elections. Areas that should be covered in such guidelines include

- cybersecurity best practices,
- background checks and other security measures for personnel,
- transparent ownership,
- processes for reporting cyber incidents, and
- supply chain integrity.

Below, we discuss the importance of each of these items, what guidelines in each of these areas could look like, and how to ensure compliance.

CYBERSECURITY BEST PRACTICES

The lead-up to the 2016 presidential election provided numerous examples of the devastating consequences of failing to heed cybersecurity best practices. Through a series of attacks that included spearphishing emails, Russian hackers gained access to internal communications of the Democratic National Committee (DNC).[47] The DNC reportedly did not install a "robust set of monitoring tools" to identify and isolate spearphishing emails on its network until April 2016, which, in retrospect, was far too late.[48] The chairman of Hillary Clinton's campaign, John Podesta, fell prey to a similar attack.[49] These threats did not end in 2016; in the run-up to the 2018 elections, hackers targeted congressional candidates including Sen. Claire McCaskill (D-MO) and Hans Keirstead, who ran in a Democratic Party primary in California.[50]

Guarding against spearphishing emails is Cybersecurity 101. Yet the numerous reports of successful spearphishing attacks suggest that many individuals and organizations fail to meet even that low bar of cyber readiness. Are vendors guarding against these (and other) attacks?[51] Special Counsel Robert Mueller's report on 2016 election interference indicates that an employee at an election vendor fell victim to a spearphishing attack, enabling malware to be installed on that vendor's network. The vendor, which many assume is VR Systems, has denied that that the attackers were able to breach its system.[52] Under the current regime, which lacks any meaningful visibility into vendors' cybersecurity practices, we simply do not, and cannot, know.

The new Technical Guidelines Development Committee should craft cybersecurity best practices that include not only equipment- and service-related offerings but also internal information technology practices, cyber hygiene, data access controls, and the like. Various bills have proposed that the TGDC take on this role, including the SAFE Act, the Election Security Act, and the For the People Act.[53]

Vulnerability to attacks by insiders is a threat **separate and apart** from a hack over the internet.

The NIST Cybersecurity Framework[54] should be the starting point and be supplemented by election-specific refinements. NIST advises that "the Framework should not be implemented as an un-customized checklist or a one-size-fits-all approach for all critical infrastructure organizations. . . . [It] should be customized by different sectors and individual organizations to best suit their risks, situations, and needs."[55]

When seeking Election Assistance Commission certification, vendors should have to demonstrate that they meet the TGDC's cybersecurity best practices. The EAC should consider providing a self-assessment handbook or other form of guidance to facilitate vendor compliance with this requirement.

Such a self-assessment handbook exists in the defense sector for contractors that handle certain sensitive information. Department of Defense contractors "that process, store or transmit Controlled Unclassified Information must meet the Defense Federal Acquisition Regulation Supplement minimum security standards" and certify that they comply with published requirements.[56] An EAC resource along these lines would provide vendors with clarity about how to assess compliance and agreed-upon metrics.

Similarly, DHS has published resources associated with its Cyber Resilience Review program, which "align[s] closely with the Cybersecurity Framework . . . developed by the National Institute of Standards and Technology."[57] They include a self-assessment package and a "Question Set with Guidance,"[58] which could prove useful in developing analogous resources for the EAC.

BACKGROUND CHECKS AND OTHER SECURITY MEASURES FOR PERSONNEL

Much of the conversation about election cybersecurity has imagined attackers in distant lands reaching our election infrastructure through the internet. But some of the most effective cyberattacks of recent years have involved insiders. To mitigate these risks, vendors should demonstrate during certification that they have sound personnel policies and practices in place.

At a minimum, vendors should describe how they screen prospective employees for security risks, including background checks, and how they assess employees for suitability on an ongoing basis, including substance-abuse screening. The Election Assistance Commission should also require vendor disclosure of controls governing staff access to sensitive election-related information. Since the bulk of such sensitive information would presumably not constitute classified information, which is subject to its own set of robust controls, the EAC's scrutiny of vendor personnel risk management will be critical.

Vulnerability to attacks by insiders is a threat separate and apart from a hack over the internet, demanding entirely different controls and defensive measures. Without adequate personnel screening and other safeguards, vendors that provide critical election services could be exposed to malfeasance from within. The FBI's thorough background checks for Justice Department attorneys and other law enforcement personnel provide a good model for aggressively vetting personnel. In the event election vendors require access to formally classified information, examples abound in the defense, nuclear, and other sectors of how to handle security clearances.

The Nuclear Regulatory Commission (NRC) regulates personnel in ways potentially relevant to election vendors.[59] Its fitness-for-duty program requires that individuals licensed to operate a nuclear reactor[60] meet several performance objectives, including "reasonable assurance" that they

- "are trustworthy and reliable as demonstrated by the avoidance of substance abuse," and
- "are not under the influence of any substance, legal or illegal, or mentally or physically impaired from

> any cause, which in any way adversely affects their ability to safely and competently perform their duties."[61]

These programs also include "reasonable measures for the early detection of individuals who are not fit to perform the duties."[62] The regulations include training requirements[63] and penalties for violations,[64] as well as robust substance-abuse testing protocols.[65] The NRC also regulates access to national security information[66] and nuclear-related restricted data[67] by individuals working for entities regulated by the commission.[68]

The defense sector also tightly circumscribes processes on personnel clearances and the handling of sensitive classified information. For example, the National Industrial Security Program Operating Manual (Department of Defense guidance on the regulation of contractors in the industrial security sector) addresses contractors' protection of such information and the processes for contractor personnel to obtain clearances.[69]

Failure to have robust and adequate personnel safeguards can lead to significant harm inflicted by those on the inside. The Swiss financial institution UBS provides a telling example. A systems administrator who worked for UBS in New Jersey, Robert Duronio, wreaked havoc on company systems after reportedly expressing dissatisfaction with his salary and bonuses. Duronio planted a "logic bomb" in UBS's systems that activated after his departure and brought down roughly 2,000 UBS computers. The attack cost the company more than $3 million in repairs, in addition to lost revenue stemming from crippled trading capability.[70] (Duronio was sentenced to 97 months in prison.)[71]

We should assume that determined foreign adversaries are capable of hiring programmers who can damage American elections. We have certainly seen foreign governments engage in similar actions against private companies. In 2006, Dongfan "Greg" Chung, a former engineer at Boeing, was arrested for hoarding trade secrets about the U.S. space shuttle program with the intent to pass this information to the Chinese government. Federal agents found sensitive documents in his home, along with journals detailing his communications with Chinese officials. Chung was convicted in 2009 of economic espionage and acting as an agent of China,[72] and sentenced to 15 years in prison.[73]

TRANSPARENT OWNERSHIP

Lack of transparency into ownership and control of election vendors can mask foreign influence over an election vendor and corruption in local certification and contracting. We recommend mandated disclosure of significant — more than 5 percent — ownership interests and a prohibition on significant foreign ownership or control (with the option to request a waiver, if certain conditions are met). The purpose is not only to deter malfeasance and corruption but also to reassure voters that the motives of election vendors are aligned with the public's interest in free and fair elections.

The threats posed by foreign influence over a U.S. election vendor — including the heightened potential for foreign infiltration of the vendor's supply chain or knowledge of client election officials' capabilities and systems — should be obvious. A federal framework for securing elections should limit significant foreign ownership of election system vendors.

Over the last several years, the topic of foreign ownership of election vendors has occasionally made headlines.[74] In 2018, the FBI informed Maryland officials that a vendor servicing the state, ByteGrid LLC, had been under the control of a Russian oligarch with close ties to President Vladimir Putin.[75] In 2019, ByteGrid sold all of its facilities and customer agreements to a company called Lincoln Rackhouse.[76]

At the same time, lack of insight into election vendor ownership presents a serious risk that vendor-led influence campaigns and public officials' conflicts of interest will escape public scrutiny. Officials might award vendor contracts in exchange for gifts or special treatment rather than to those that would best facilitate free and fair elections. Transparency into ownership and control is required for the public to assess whether officials engaged in procurement and regulation have been improperly influenced.

There are a range of approaches to these problems of improper foreign and domestic influence. We recommend a stringent yet flexible standard: a requirement to disclose all entities or persons with a greater than 5 percent ownership or control interest, along with a ban on foreign ownership in that same amount,[77] with an option for the EAC to grant a waiver after consultation with DHS. While this proposal would address instances of foreign control over election vendors, such as ByteGrid, it could also impact companies such as Dominion Voting Systems, the second-largest voting machine vendor in the United States, whose voting machines are used by more than one-third of American voters and whose headquarters are in Toronto. Similarly, Scytl Secure Electronic Voting, which offers election night reporting and other election technologies to hundreds of election jurisdictions around the United States, is based in Barcelona.[78] A waiver would provide a means for these and other vendors with foreign ties to disclose those relationships and put in place safeguards to prevent foreign influence and alleviate security concerns, thus offering a reasonable path for a wide range of vendors to participate in the election technology market. Beyond this initial disclosure requirement, vendors should have an ongoing obligation to notify their customers and the EAC of any subsequent changes in their ownership or control.

The EAC can look to other sectors for examples of vendor disclosure of ownership or control agreements.

The Department of Defense's National Industrial Security Program Operating Manual is instructive. It requires companies to "complete a Certificate Pertaining to Foreign Interests when . . . significant changes occur to information previously submitted,"[79] and it requires vendors to submit reports when there is "any material change concerning the information previously reported by the contractor concerning foreign ownership control or influence."[80]

Lawmakers have already introduced legislation to improve transparency in ownership or control of election system vendors, with mechanisms ranging from disclosure requirements to strict bans on foreign ownership or control. One approach recently adopted in North Carolina requires disclosure of all owners with a stake of 5 percent or more in a vendor's company, subsidiary, or parent, so that the state's Board of Elections can consider this information before certifying a voting system.[81]

On the other end of the spectrum, the For the People Act and the SAFE Act would require that vendors in states receiving federal grants be owned and controlled by U.S. citizens or permanent residents, with no option for a waiver.[82] Similarly, the Election Vendor Security Act would have required each vendor to certify that "it is owned and controlled by a citizen, national, or permanent resident of the United States, and that none of its activities are directed, supervised, controlled, subsidized, or financed, and none of its policies are determined by, any foreign principal" or agent.[83]

Both the public and local and state governments are often **kept in the dark** about security breaches.

Other proposals would prohibit foreign control but provide for a waiver, as we suggest. For instance, the Protect Election Systems from Foreign Control Act would require vendors to be "solely owned and controlled by a citizen or citizens of the United States" absent a waiver.[84] Such waivers could be granted if the vendor "has implemented a foreign ownership, control, or influence mitigation plan that has been approved by the [DHS] Secretary . . . ensur[ing] that the parent company cannot control, influence, or direct the subsidiary in any manner that would compromise or influence, or give the appearance of compromising or influencing, the independence and integrity of an election."[85]

With respect to defining an ownership or control interest of greater than 5 percent, the EAC could borrow from the approach used by the Federal Communications Commission (FCC). The FCC typically defines foreign ownership, including indirect ownership, by multiplying the percentage of shares an owner has in one company by the percentage of shares that company owns in a regulated broadcast or common carrier licensee. For instance, if a foreign person owned 30 percent of company A, and company A owned 25 percent of company B, the foreign person would be deemed to own 7.5 percent of company B. For purposes of voting shares, the FCC treats a majority stake as 100 percent, whereas for equity shares, the actual percentages are used.[86]

PROCESSES FOR REPORTING CYBER INCIDENTS

Both the public and local and state governments are often kept in the dark about security breaches that affect election vendors. This state of affairs can undermine faith in the vote and leave election officials unsure about vendor vulnerabilities. To address these concerns, vendors should face robust incident reporting requirements and a mandate to work with affected election authorities.

Federal oversight should require vendors to agree to report security incidents as a condition of certification. The Election Assistance Commission should require that vendors report to it and to all potentially impacted jurisdictions within days of discovering an incident. The EAC's existing Quality Monitoring Program requires only that vendors with certified voting equipment "submit reports of any voting system irregularities."[87] At present, the reporting requirement extends only to vendors of voting systems and does not encompass any other facets of those vendors' services, equipment, or operations. Election officials have long complained that vendors do not always share reports of problems with their systems.[88] Compounding the problem, a single vendor often serves many jurisdictions.[89]

Some legislation has already sought to mandate more fulsome incident reporting by vendors. The Secure Elections Act, which had bipartisan support before losing momentum in 2018, included a mandatory reporting provision. Under the bill, if a so-called election service provider has "reason to believe that an election cybersecurity incident may have occurred, or that an information security incident related to the role of the provider as an election service provider may have occurred," then it must "notify the relevant election agencies in the most expedient time possible and without unreasonable delay (in no event longer than 3 calendar days after discovery of the possible incident)" and "cooperate with the election agencies in providing [their own required notifications]."[90]

Absent robust incident reporting, election officials and the public can be left unaware of potential threats that vendors might introduce into elections. As previously discussed, there is still considerable uncertainty concerning the alleged spearphishing attack and hack of a vendor involved in the 2016 elections. Much of what is known stems from the leak of a classified intelligence report obtained by the *Intercept*,[91] which identified the hacking victim as a Florida-based vendor, coupled with Special Counsel Robert Mueller's report to the attorney general and indictment of 12 Russian intelligence officers.[92] Further complicating the picture of what happened, the Florida-based vendor, VR Systems, responded to an inquiry from Sen. Ron Wyden (D–OR) via letter, claiming that "based on our internal review, a private sector cyber security expert forensic review, and the DHS review, we are confident that there was never an intrusion in our EViD servers or network."[93] This uncertainty offers little for the vendor's clients to rely on in assessing the vendor's ongoing cyber readiness and whether to continue to contract with the vendor in future elections.

With mandated incident reporting, the EAC could provide the necessary assurance to election officials regarding the security of vendors by sharing information with election officials who need it, as well as by requiring appropriate remedial action, up to and including decertification.

SUPPLY CHAIN INTEGRITY

Federal regulators should require vendors to follow best practices for managing supply chain risks to election security. The new Technical Guidelines and Development Committee should define categories of subcontractors or products that pose serious risks, such as servers and server hosting, software development, transportation of sensitive equipment such as voting machines, and information storage. For instance, Liberty Systems, one of Unisyn Voting Solutions' regional partners, would likely be covered, given that it "provides election and vital statistics, software, and support throughout counties in the State of Illinois."[94] The TGDC's guidelines could then require that vendors have a framework to ensure that high-risk subcontractors and manufacturers also follow best practices on cybersecurity, background checks, and foreign ownership and control, as well as reporting cyber incidents to the vendor.

This approach is being used in other areas of government, where a growing recognition of supply chain risk to national security exists. The Department of Defense has recently stepped up its enforcement of supply chain integrity and security standards, requiring review of prime contractors' purchasing systems to ensure that Department of Defense contractual requirements pertaining to covered defense information and cyber incident reporting "flow down appropriately to . . . Tier 1 level suppliers" and that prime contractors have procedures in place for assessing suppliers' compliance with those requirements.[95]

The Department of Defense now requires that contractors handling controlled unclassified information (CUI) "flow down" contractual clauses to subcontractors whose "performance will [also] involve [the department's] CUI." The TGDC should develop an analogous category of subcontractors and manufacturers for which the same cybersecurity, background check requirements, and foreign ownership concerns that apply to election vendors would apply, based on the subcontractor's role and the opportunity for election security risk to be introduced.

Monitoring Vendor Compliance

To make its oversight most effective, the Election Assistance Commission must have the ability to confirm that federally certified vendors continue to meet their obligations. The fact that a vendor was, at some point in time, certified as meeting relevant federal standards is no guarantee that circumstances have not changed. Failure to stay in compliance should lead to appropriate remedial action by the EAC, up to and including decertification.

The EAC's Quality Monitoring Program for voting systems provides a starting point for how this might work. The EAC offers a mechanism for election officials on the ground to provide information about any voting system anomalies present in certified voting machines. If an election worker submits a credible report of an anomaly, the EAC distributes it to state and local election jurisdictions with similar systems, the manufacturer of the voting system, and the testing lab that certified the voting system.[96] According to the EAC's certification manual, "the Quality Monitoring Program is not designed to be punitive but to be focused on improving the process."[97] The program, then, is focused more on compliance than certification or decertification, although decertification can result in cases of persistent noncompliance.

The SAFE Act and the For the People Act call for the testing of voting systems nine months before each federal general election, as well as for the decertification of systems that do not meet current standards.[98]

A critical difference between the ability to monitor voting equipment and the practices of an election system vendor is that thousands of election officials and poll workers, and hundreds of millions of voters, interact with voting equipment on a regular basis. They can report anomalies when they see them. By contrast, most of the work of election system vendors happens out of public view.

For this reason, vendors must be obligated on an ongoing basis to remedy known security flaws or risk losing federal certification. Congress should provide the EAC with a mandate to ensure that vendors contract with independent security firms to conduct regular audits, penetration testing, and physical inspections and site visits, and to provide the results of those assessments to the EAC. One legislative proposal — the Protect Election Systems from Foreign Control Act — sought to do something similar by subjecting vendors to an annual evaluation to assess compliance with cybersecurity best practices.[99] The EAC's effectiveness in its new oversight role would be diminished absent some power to monitor vendors' efforts on this front — a power Congress ought to provide.

The EAC could require regular penetration testing by third parties to assess vendors' cyber readiness in real time. Such testing would give the EAC (and vendors) an opportunity to identify and remediate security flaws, hopefully before adversaries take advantage of them. The EAC should also consider using bug bounty programs, which have become a common tool deployed by private industry and government entities, including the Department of Defense.[100] Under bug bounty programs, friendly so-called white-hat hackers earn compensation for reporting vulnerabilities and risks to program sponsors. The For the People Act calls for such a program,[101] as does the Department of Justice's Framework for a Vulnerability Disclosure Program for Online Systems.[102]

Certified vendors should be required to submit to extensive inspection of their facilities. To assess compliance with cybersecurity best practices, personnel policies, incident reporting and physical security requirements, and the like, the EAC must be granted wide latitude to demand independent auditors' access to vendor systems and facilities. This should include unannounced, random inspections of vendors. The element of surprise could serve as a powerful motivator for vendors to stay in compliance with EAC guidance.

The Defense Contract Management Agency (DCMA) performs an analogous, if broader, role for military contractors. Serving as the Defense Department's "information brokers and in-plant representatives for military, Federal, and allied government buying agencies," DCMA's duties extend to both "the initial stages of the acquisition cycle and throughout the life of the resulting contracts."[103] In that latter stage of a contract, DCMA monitors "contractors' performance and management systems to ensure that cost, product performance, and delivery schedules are in compliance with the terms and conditions of the contracts."[104] This function includes having personnel in contractor facilities assess performance and compliance.[105] Although our proposal does not envision the EAC performing an ongoing contract compliance role, the EAC's enhanced oversight role could take some cues from DCMA's inspection protocols and ability to closely scrutinize vendors.

The NRC similarly holds inspection rights over those subject to its regulations, including companies that handle nuclear material and those holding licenses to operate power plants.[106] The NRC regulation requiring that those regulated "afford to the Commission at all reasonable times opportunity to inspect materials, activities, facilities, premises, and records under the regulations in this chapter" is of particular relevance to potential EAC oversight.[107] The NRC also has an extensive set of regulations concerning physical security at nuclear sites and of nuclear material.[108] Although these requirements are probably more onerous than those needed in the election sector (especially since nuclear material poses unique physical security risks), they could nonetheless prove instructive in crafting physical security requirements for vendors. Such requirements should go hand in hand with the cybersecurity best practices discussed above.

Enforcing Guidelines

It is critical to have a clear protocol for addressing election system vendor violations of federal guidelines. If states require their election offices to use only federally certified vendors, revocation of federal certification could have a potentially devastating impact on the ability of jurisdictions to run elections and ensure that every voter is able to cast a ballot.

Again, the Election Assistance Commission's process for addressing anomalies in voting equipment through its Quality Monitoring Program is instructive. If it finds that a system is no longer in compliance with the VVSG, the manufacturer is sent a notice of noncompliance. This is not a decertification of the machine but rather a notification to the manufacturer of its noncompliance and its procedural rights before decertification. The manufacturer has the right to present information, access the information that will serve as the basis of the decertification decision, and cure system defects prior to decertification. The right to cure system defects is limited; it must be done before any individual jurisdiction that uses the system next holds a federal election.[109]

If decertification moves forward after attempts to cure or opportunities to submit additional information, the manufacturer may appeal the decision. If the appeal is denied, then the decertified voting system will be treated as any other uncertified system. The EAC will also notify state and local election officials of the decertification.[110] A decertified system may be resubmitted for certification and will be treated as any other system seeking certification.

The EAC's application of this process to the ES&S voting system Unity 3.2.0.0 provides an example of how this can happen. Certification of this system was granted in 2009.[111] In 2011, the EAC's Quality Monitoring Program received information about an anomaly in the system and began a formal investigation.[112] A notice of noncompliance was then sent to ES&S in 2012, listing the specific anomalies found in the voting system and informing ES&S that if these anomalies were not remedied, the EAC would be obligated to decertify the voting system.[113] ES&S attempted to cure the defects, as was its right, and produced a new, certified version of the Unity system.[114] The vendor then requested that its old system be withdrawn from the list of EAC certified systems.[115]

Decertification of a vendor would need to be handled thoughtfully, so that local election officials are not left scrambling to contract new election services close to an election. In this sense, close coordination among federal and local officials and relevant vendors to proactively identify and fix issues would be necessary for any scheme to succeed. The EAC would also have to be left with the flexibility to decide what, if any, equipment and services could no longer be used or sold as federally certified. To that end, decertification should incorporate these key elements:

- A voting system decertification should not necessarily result in a vendor decertification and vice versa. For instance, a voting machine vendor might be found to be out of compliance with federal requirements for background checks on employees. If the EAC determines this noncompliance did not impact the security of voting machines already in the field, it could leave the voting system certified but ban the vendor from selling additional machines (or certain employees from servicing existing machines) until the failure is remedied. Alternatively, it could allow the vendor's voting machines to continue to be used for a limited time, subject to additional security measures, such as extra preelection testing and postelection audits.
- There should be a clear process ahead of a formal decertification, with notification to affected state and local officials and plenty of opportunities for the relevant vendor to address issues before the EAC takes more drastic action. Only the most urgent and grave cybersecurity lapses should truncate this decertification process.
- Any decertification order should include specific guidance to state and local officials on how existing vendor products or services are affected, assistance to those officials with replacing those goods or services (if necessary), and a road map for the vendor to regain certification.

Conclusion

Private election vendors play a crucial role in securing the nation's elections against malicious actors who have already taken steps toward compromising elections and the public's confidence in our democracy. Yet these vendors are currently subject to little oversight to ensure that they remain secure against these threats and that many of the products and services they provide, such as electronic pollbooks, are secure. Currently, only voting systems — the systems used to cast and tabulate ballots — are subject to robust federal oversight, and then only via a voluntary certification program. We recommend that Congress empower the Election Assistance Commission to certify election vendors more broadly as compliant with voluntary guidelines relating to cybersecurity, personnel, transparent ownership and control, reporting of cyber incidents, and supply chain integrity. In the meantime, the EAC should employ its registration and certification processes to ensure that vendors of certified voting systems keep up with these practices.

Endnotes

[1] Kim Zetter, "The Crisis of Election Security," *New York Times Magazine*, Sept. 26, 2018, https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html.

[2] The For the People Act, H.R. 1, 116th Cong. (2019) and the Securing America's Federal Elections Act, the SAFE Act, H.R. 2722, 116th Cong. (2019) both would accomplish much, but not all, of this report's recommendations. Specifically, these bills provide for EAC oversight of a broader array of election system products and vendors in exchange for receipt and use of federal funds but do not provide for ongoing certification and monitoring of vendors. They also do not speak to best practices on personnel decisions or supply chain security. These bills also do not fully address how to define foreign ownership and control. Where this report's recommendations could be accomplished by adopting one of these bills, we have attempted to flag that for the reader.

[3] Compare, for example, The Labeling of Hazardous Art Materials Act, 15 U.S.C. 1277, and 16 C.F.R. §§ 1500.14, with 11 CFR §§ 9405.1 et seq. Indeed, Chapter II of Title 11 of the Code of Federal Regulations, the principal regulations applicable to the EAC, does not address the certification of voting systems or any potential oversight of election vendors more broadly. Nor does the legislation that established the EAC (the Help America Vote Act of 2002) — which sets some requirements for voting systems used in federal elections, see 52 U.S.C. § 21081 — require the EAC to issue any mandatory regulations on those topics. See, e.g., 52 U.S.C § 20971 (regarding the certification and testing of voting systems), § 20929 ("The Commission shall not have any authority to issue any rule, promulgate any regulation, or take any other action which imposes any requirement on any State or unit of local government . . ."), § 21101 (regarding the EAC's adoption of *voluntary* guidance).

[4] *Hearing on Election Security, Before the Comm. on House Administration*, 116th Cong. (May 8, 2019) (statement of Zoe Lofgren, chairperson).

[5] *Hearing on Election Security, Before the Comm. on House Administration*, 116th Cong. (May 8, 2019) (statement of John Merrill, Alabama secretary of state).

[6] U.S. Senate Select Committee on Intelligence, *Report of the Select Committee on Intelligence, U.S. Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 1*, July 5, 2019, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf ("State election officials, who have primacy in running elections, were not sufficiently warned or prepared to handle an attack from a hostile nation-state actor."); U.S. Const. art. I, § 4 (permitting Congress to regulate elections); U.S. Const. art. IV, § 4 (requiring Congress to guarantee a republican form of government to the states and to protect them from invasion).

[7] Lorin Hitt et al., *The Business of Voting: Market Structure and Innovation in the Election Technology Industry*, University of Pennsylvania Wharton School, 2017, 15, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

[8] Frank Bajak, "US Election Integrity Depends on Security-Challenged Firms," Associated Press, Oct. 29, 2018, https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c (quoting Sen. Ron Wyden).

[9] Hitt et al., *The Business of Voting*, 7.

[10] Hitt et al., *The Business of Voting*, 8.

[11] U.S. Senate Select Committee on Intelligence, *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations*, May 8, 2018, https://www.intelligence.senate.gov/publications/russia-inquiry.

[12] United States v. Netyksho et al., No. 1:18CR00215, 2018 WL 3407381, 26 (D.D.C. Jul. 13, 2018); Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election, U.S. Department of Justice, 2019, 50*, https://www.justice.gov/storage/report.pdf; Casey Tolan, "Humboldt County Shores Up Voting Systems after Russian Hack of Election Contractor," *Mercury News*, June 6, 2017, https://www.mercurynews.com/2017/06/06/humboldt-county-moves-to-shore-up-voting-systems-after-election-contractor-hack (listing VR Systems' own website as the source for its list of states in which the company operates).

[13] Sam Biddle, "A Swing-State Election Vendor Repeatedly Denied Being Hacked by Russians. The New Mueller Indictment Says Otherwise," *Intercept*, July 13, 2018, https://theintercept.com/2018/07/13/a-swing-state-election-vendor-repeatedly-denied-being-hacked-by-russians-new-mueller-indictment-says-otherwise.

[14] United States v. Netyksho et al., No. 1:18CR00215, 2018 WL 3407381, 26 (D.D.C. Jul. 13, 2018).

[15] Miles Parks, "Florida Governor Says Russian Hackers Breached Two 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.

[16] Kim Zetter, "Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials," *Vice*, Aug. 8, 2019, https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials (quoting ES&S marketing literature).

[17] Dan O'Sullivan, "The Chicago Way: An Electronic Voting Firm Exposes 1.8M Chicagoans," *Upguard*, Dec. 13, 2018, https://www.upguard.com/breaches/cloud-leak-chicago-voters.

[18] Bajak, "US Election Integrity."

[19] "Report Blames Software Error for Los Angeles Voting Problem," Associated Press, Aug. 1, 2018, https://www.apnews.com/95b056ab2eab47febaf721a1d285a045; IBM Security Services, *Independent Investigation of Election System Anomalies in Los Angeles County on June 5, 2018*, Aug. 1, 2018, http://file.lacounty.gov/SDSInter/lac/1042885_FINALExecutiveSummaryAugust12018.pdf; See also Board of Supervisors, *Request for Approval: Amendment Number Eight to Agreement Number 76010 with Data Information Management Systems, LLC for Voter Information Management System Maintenance and Support Services*, County of Los Angeles, 2015, https://www.lavote.net/documents/05052015.pdf (identifying ES&S subsidiary Data Information Management Systems, LLC, as vendor responsible for maintaining and servicing Los Angeles County's voter information management system).

[20] U.S. Election Assistance Commission, "Quality Monitoring Program," https://www.eac.gov/voting-equipment/quality-monitring-program.

[21] National Protection and Programs Directorate, "DHS and Private Sector Partners Establish Information and Communications Technology Supply Chain Risk Management Task Force," U.S. Department of Homeland Security, Oct. 30, 2018, https://www.dhs.gov/news/2018/10/30/dhs-and-private-sector-partners-establish-information-and-communications-technology.

[22] See, e.g., Sean Keane, "Huawei Ban: Full Timeline on How and Why Its Phones Are Under Fire," *CNET*, May 30, 2019, https://www.cnet.com/news/huawei-ban-full-timeline-on-how-and-why-its-phones-are-under-fire.

[23] Unisyn Voting Systems, "Partners," https://unisynvoting.com/partners.

[24] The EAC's bipartisan structure provides important checks and balances, but it also carries a risk of the sort of pervasive gridlock that has hamstrung the Federal Election Commission, leading the Brennan Center to advocate for a fundamental overhaul of that agency. See Daniel I. Weiner, *Fixing the FEC: An Agenda for Reform, Brennan Center for Justice*, 2019, https://www.brennancenter.org/sites/default/files/publications/2019_04_FECV_Final.pdf. But the EAC's mission is very different from that of the FEC, which oversees campaign finance.

Because of the technical nature of much of its work, the EAC has not been paralyzed by the same partisan ideological divisions, leading us to conclude that its bipartisan structure remains viable, at least for now.

25 Ian Urbina, "Panel Said to Alter Finding on Voter Fraud," *New York Times*, Apr. 11, 2007, https://www.nytimes.com/2007/04/11/washington/11voters.html.

26 Eric Geller, "Federal Election Official Accused of Undermining His Own Agency," *Politico*, June 15, 2019, https://www.politico.com/story/2019/06/15/federal-election-brian-newby-2020-1365841.

27 Kim Zetter, "Experts: Elections Commission Downplaying Unseen Risks to 2020 Vote," *Politico*, Mar. 15, 2019, https://www.politico.com/story/2019/03/15/election-machine-security-2020-cybersecurity-1222803.

28 Geller, "Federal Election Leader Accused."

29 U.S. Election Assistance Commission, *Fiscal Year 2019 Congressional Budget Justification*, Feb. 12, 2018, https://Www.Eac.Gov/Assets/1/6/Fy_2019_Cbj_Feb_12_2018_Final.Pdf; Omnibus Appropriations Act, 2009, Pub. L. No. 111-8 (2009); Election Assistance Commission Termination Act, H.R. Rept. 114-361 (2015).

30 Both the House and Senate held EAC oversight hearings this year, but they were the first oversight hearings in either chamber in over eight years. See Committee on House Administration, "Hearings," https://cha.house.gov/committee-activity/hearings; "Congressional Hearings," Govinfo, https://www.govinfo.gov/app/collection/chrg/116/house/Committee%20on%20House%20Administration; Senate Committee on Rules and Administration, "Hearings," https://www.rules.senate.gov/hearings.

31 Under the Help America Vote Act, Pub. L. No. 107-252 (2002), this includes all equipment that is used to "define ballots; . . . cast and count votes; . . . report or display election results; and . . . maintain and product any audit trail information." It does not include certification of other election systems, such as electronic pollbooks; such machines are now used widely and are critical to running elections around the country. See Andrea Cordova, "Want a Simple Way to Increase Election Security? Use Paper," Brennan Center for Justice, Oct. 8, 2018, https://www.brennancenter.org/blog/want-simple-way-increase-election-security-use-paper. They, too, should be added to this system testing regime, as was proposed recently in the Election Security Assistance Act, H.R. 3412, 116th Cong. (2019), § 3(a) .

32 The EAC can conduct manufacturing site visits through its Quality Monitoring Program, but a site visit is unlikely to uncover insecure development practices, which can pose problems at later stages, such as during the provision of technical support to election officials or the programming of a ballot style or candidate register.

33 For the People Act, H.R. 1, 116th Cong. (2019), § 3302; Securing America's Federal Elections Act, H.R. 2722, 116th Cong. (2019), § 204; Election Security Assistance Act, H.R. 3412, 116th Cong. (2019), § 3(a).

34 U.S. Election Assistance Commission, *Voluntary Voting System Guidelines*, Vol. 1, Version 1.1, 2015, https://www.eac.gov/assets/1/28/VVSG.1.1.VOL.1.FINAL1.pdf.

35 U.S. Election Assistance Commission, *VVSG Public Hearing (Apr. 10, 2019)* (statement of Vice Chairman Ben Hovland).

36 U.S. Election Assistance Commission, *Testing and Certification Program Manual, Version 2.0, 2015, 71*, https://www.eac.gov/assets/1/6/Cert_Manual_7_8_15_FINAL.pdf.

37 *Testing and Certification Program Manual, Version 2.0, EAC, 71-75.*

38 Election Vendor Security Act, H.R.6435, 115th Cong. (2018).

39 For the People Act, H.R. 1, 116th Cong. (2019), § 298A; Securing America's Federal Elections Act, H.R. 2722, 116th Cong. (2019), § 297A.

40 U.S. Election Assistance Commission, "Fact Sheet: The U.S. Election Assistance Commission's Voting System Testing and Certification Program," Mar. 7, 2017, https://www.eac.gov/news/2017/03/07/fact-sheet-the-us-election-assistance-commissions-voting-system-testing-and-certification-program-voting-systems-certification-communications-fact-sheet.

41 U.S. Department of Homeland Security, *Election Infrastructure Subsector Coordinating Council Charter*, Version 1.0, 2018, 3, https://www.dhs.gov/sites/default/files/publications/govt-facilities%20-EIS-scc-charter-2018-508.pdf.

42 When the TGDC advised a restructuring of the VVSG in 2007, its recommendations were never adopted. Work began on a "patch," the VVSG 1.1, but that was halted for years, when the EAC lost a quorum, and was ultimately adopted only in 2015. A new VVSG 2.0 was provided by the TGDC in Feb. 2017 and was recommended for adoption that September, but again the EAC lost its quorum. It is now out for public comment. U.S Election Assistance Commission, VVSG Public Hearing Apr. 10, 2019) (statement of Ryan Macias), https://www.eac.gov/events/2019/04/10/vvsg-public-hearing.

43 U.S. Election Assistance Committee, "Technical Guidelines Development Committee," https://www.eac.gov/about/technical-guidelines-development-committee/.

44 Voting System Cybersecurity Act of 2019, S. 1454, 116th Cong. (2019), § 2.

45 A possible configuration of the NIST-chosen representatives could be

- one representative from CISA with technical and scientific expertise related to cybersecurity in election technology;
- one representative of state election information technology directors selected by the National Association of State Election Directors;
- one representative from the National Association of State Chief Information officers (NACIO) with expertise in cybersecurity;
- one representative from the EI-ISAC with technical and scientific expertise related to cybersecurity in elections;
- two representatives who are academic or scientific researchers with technical and scientific expertise related to cybersecurity, chosen by NIST;
- one representative who possesses technical and scientific expertise relating to the accessibility and usability of voting systems, chosen by NIST;
- one representative of manufacturers of voting system hardware and software who possesses technical and scientific expertise relating to cybersecurity and the administration of elections, selected jointly by the EAC and NIST; and
- one representative of a laboratory accredited under section 231(b) who possesses technical and scientific expertise relating to cybersecurity and the administration of elections, selected by the NIST National Voluntary Laboratory Assessment Program (NVLAP).

A similar proposal to modify the TGDC appears in S. Amdt. 3983 to H.R. 6157, 115th Cong. (2018).

46 Currently, guidelines issued by the TGDC do not go into effect absent approval by the EAC, which can create significant delays, and voting system vendors have obtained certification to older versions of the VVSG, even after new versions have been approved by the EAC. See Tim Starks, "EAC Finally Nearing Ability to Take Major Action," *Politico*, Nov. 28, 2018, https://www.politico.com/newsletters/morning-cybersecurity/2018/11/28/eac-finally-nearing-ability-to-take-major-action-433181 (describing the EAC's lack of a quorum since March 2018, which prevented it from approving a new version of the VVSG). See U.S. Election Assistance Commission, "Certified Voting Systems," https://www.eac.gov/voting-equipment/certified-voting-systems (showing voting systems as certified in 2017, 2018, and 2019 to VVSG 1.0, a set of guidelines that was replaced by VVSG 1.1 in 2015).

47 Philip Bump, "Timeline: How Russian Agents Allegedly Hacked the DNC and Clinton's Campaign," *Washington Post*, July 13, 2018, https://www.washingtonpost.com/news/politics/wp/2018/07/13/timeline-how-russian-agents-allegedly-hacked-the-dnc-and-clintons-campaign/?utm_term=.618a5496022b; Eric Lipton, David E. Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *New York Times*, Dec. 13, 2016, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

48 Lipton et al., "The Perfect Weapon."

[49] Lipton et al., "The Perfect Weapon."

[50] Eric Geller, "Microsoft Reveals First Known Midterm Campaign Hacking Attempts," *Politico*, July 19, 2018, https://www.politico.com/story/2018/07/19/midterm-campaign-hacking-microsoft-733256; Kevin Poulsen and Andrew Desiderio, "Russian Hackers' New Target: A Vulnerable Democratic Senator," *Daily Beast*, July 26, 2018, https://www.thedailybeast.com/russian-hackers-new-target-a-vulnerable-democratic-senator; Andy Kroll, "Documents Reveal Successful Cyberattack in California Congressional Race," *Rolling Stone*, Aug. 15, 2018, https://www.rollingstone.com/politics/politics-news/california-election-hacking-711202.

[51] Using remote-access software to access a computer risks opening up access to the entire network that computer is connected to. Yet it has been alleged that VR systems used such software in 2016 to connect to the North Carolina State Board of Elections, in order to download a voter list for Durham County. Kim Zetter, "Software Vendor May Have Opened a Gap for Hackers in 2016 Swing State," *Politico*, June 5, 2019, https://www.politico.com/story/2019/06/05/vr-systems-russian-hackers-2016-1505582.

[52] Mueller, *Report on the Investigation into Russian Interference*, 51; Kim Zetter, "Florida Election Vendor Says It Has Proof It Wasn't Breached by Russians," *Politico*, May 23, 2019, https://www.politico.com/story/2019/05/23/florida-vendor-russia-1469086.

[53] Securing America's Federal Elections Act, H.R. 2722, 116th Cong. (2019), § 297A; Election Security Act, H.R. 2660, 116th Cong. (2019), § 297A; Election Security Act of 2019, S. 1540, 116th Cong. (2019), § 297A; For the People Act, H.R. 1, 116th Cong. (2019), § 298A.

[54] National Institute of Standards and Technology, "Cybersecurity Framework," https://www.nist.gov/cyberframework.

[55] National Institute of Standards and Technology, "Questions & Answers," https://www.nist.gov/cyberframework/questions-and-answers#checklist.

[56] Patricia Toth, *NIST Handbook 162: NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements*, National Institute for Standards and Technology, 2017, https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf. See also, "DFARS Cybersecurity Requirements," Manufacturing Extension Partnership, National Institute of Standards and Technology, created Dec. 1, 2017, updated June 28, 2018, https://www.nist.gov/mep/cybersecurity-resources-manufacturers/dfars800-171-compliance.

[57] U.S. Department of Homeland Security, "Cyber Resilience Review," https://www.us-cert.gov/sites/default/files/c3vp/crr-fact-sheet.pdf.

[58] See generally U.S. Department of Homeland Security, "Cybersecurity Framework," Critical Infrastructure Cyber Community Voluntary Program, https://www.us-cert.gov/ccubedvp/cybersecurity-framework.

[59] U.S. Nuclear Regulatory Commission, "About NRC," last updated Feb. 12, 2018, https://www.nrc.gov/about-nrc.html.

[60] See generally, 10 C.F.R. §§ 26.1–26.825.

[61] 10 C.F.R. § 26.23.

[62] 10 C.F.R. § 26.23.

[63] 10 C.F.R. § 26.29.

[64] 10 C.F.R. §§ 26.181–26.189.

[65] 10 C.F.R. §§ 26.81–26.119.

[66] 10 C.F.R. § 10.5 ("*National Security Information* means information that has been determined under Executive Order 13526 or any predecessor or successor order to require protection against unauthorized disclosure and that is so designated.").

[67] 10 C.F.R. § 10.5 ("*Restricted Data* means all data concerning design, manufacture, or utilization of atomic weapons, the production of special nuclear material, or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 142 of the Atomic Energy Act of 1954, as amended.").

[68] 10 C.F.R. § 10.1(a) ("This part establishes the criteria, procedures, and methods for resolving questions concerning:...(3) The eligibility of individuals who are employed by or are applicants for employment with NRC licensees, certificate holders, holders of standard design approvals under part 52 of this chapter, applicants for licenses, certificates, and NRC approvals, and others who may require access related to a license, certificate, or NRC approval, or other activities as the Commission may determine, for access to Restricted Data under the Atomic Energy Act of 1954, as amended, and the Energy Reorganization Act of 1974, or for access to national security information.").

[69] National Industrial Security Program, *Operation Manual, Feb. 2006*, §§ 2-200–2-211, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf.

[70] U.S. Department of Justice, "Disgruntled UBS PaineWebber Employee Charged with Allegedly Unleashing 'Logic Bomb' on Company Computers," Dec. 17, 2002, https://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/duronioIndict.htm; Stephen Foley, "Disgruntled Worker 'Tried to Cripple UBS in Protest over $32,000 Bonus'," *Independent*, June 8, 2006, https://www.independent.co.uk/news/business/news/disgruntled-worker-tried-to-cripple-ubs-in-protest-over-32000-bonus-481515.html.

[71] Ericka Chickowski, "Former UBS System Administrator Gets Eight Years for Logic Bomb," *SC Media*, Dec. 18, 2006, https://www.scmagazineuk.com/article/1467247.

[72] U.S. Department of Justice, "Former Boeing Engineer Convicted of Economic Espionage in Theft of Space Shuttle Secrets for China," July 16, 2009, https://www.justice.gov/opa/pr/former-boeing-engineer-convicted-economic-espionage-theft-space-shuttle-secrets-china.

[73] "Chinese-Born Engineer Gets 15 Years for Spying," Associated Press, Feb. 8, 2010, http://www.nbcnews.com/id/35300466/ns/us_news-security/t/chinese-born-engineer-gets-years-spying/#.XUrYm-hKg2w.

[74] For example, there were reports that Venezuelan interests with ties to the Venezuelan government owned the parent company of an election vendor, Sequoia Voting Systems, which Dominion later acquired. See Tim Golden, "U.S. Investigates Voting Machines' Venezuela Ties," *New York Times*, Oct. 29, 2006, https://www.nytimes.com/2006/10/29/washington/29ballot.html. The Venezuelan owners of Sequoia's parent company eventually agreed to sell Sequoia. See Zachary A. Goldfarb, "U.S. Drops Inquiry of Voting Machine Firm," *Washington Post*, Dec. 23, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/12/22/AR2006122201304.html.

[75] Mark Morales, "Maryland Election Contractor Has Ties to Russian Oligarch," CNN, July 16, 2018, https://www.cnn.com/2018/07/16/politics/maryland-elections-russia/index.html; Chase Cook and E.B. Furgurson III, "FBI Informs Maryland of Election Software Owned by Russian Firm, No Known Breaches," *Capital Gazette*, July 13, 2018, https://www.capitalgazette.com/news/government/ac-cn-russian-election-0714-story.html.

[76] Rich Miller, "Lincoln Rackhouse Continues Expansion With Purchase of ByteGrid," *Data Center Frontier*, May 8, 2019, https://datacenterfrontier.com/lincoln-rackhouse-continues-expansion-with-purchase-of-bytegrid.

[77] We recommend defining "foreign national" as someone who is neither a U.S. citizen nor a U.S. permanent resident, as this is the definition used by the FEC in prohibiting foreign contributions to candidates.

[78] Jordan Wilkie, "'They Think They Are Above the Law': The Firms that Own America's Voting System," *Guardian*, Apr. 23, 2019, https://www.theguardian.com/us-news/2019/apr/22/us-voting-machine-private-companies-voter-registration; Hitt et al., *The Business of Voting*; Scytl, "US Elections," https://www.scytl.com/en/customers/us-elections.

[79] National Industrial Security Program, *Operation Manual*, Feb. 2006, § 2-302, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf.

[80] National Industrial Security Program, *Operation Manual*, **§1-**

302(g)(5).

81 North Carolina Board of Elections, *Election Systems Certification Program*, amended June 2019, 3–20, https://s3.amazonaws.com/dl.ncsbe.gov/State_Board_Meeting_Docs/2019-06-13/Voting%20System%20Certification/NCSBEVotingSystemsCertificationProgram_06132019.pdf; Ben Popken, "State Officials Demand Voting System Vendors Reveal Owners after Russian Hacks and Investments," NBC News, June 24, 2019, https://www.nbcnews.com/politics/elections/voting-system-vendors-reveal-owners-after-russian-hacks-investments-n1020956.

82 For the People Act, H.R. 1, 116th Cong. (2019), § 298A; Securing America's Federal Elections Act, H.R. 2722, 116th Cong. (2019), § 297A.

83 Election Vendor Security Act, H.R. 6435, 115th Cong. (2018).

84 Protect Election Systems from Foreign Control Act, H.R. 6449, 115th Cong. (2018).

85 Protect Election Systems from Foreign Control Act, H.R. 6449, 115th Cong. (2018).

86 In Review of Foreign Ownership Policies for Broadcast, Common Carrier and Aeronautical Radio Licensees under Section 310(b)(4) of the Communications Act of 1934, as Amended, FCC 16-128, §1.5001(f) (Sept. 29, 2016).

87 U.S. Election Assistance Commission, "Frequently Asked Questions: Voting System Certification Questions," https://www.eac.gov/voting-equipment/frequently-asked-questions.

88 Lawrence Norden, *Voting System Failures: A Database Solution*, 2010, 9, https://www.brennancenter.org/sites/default/files/legacy/Democracy/Voting_Machine_Failures_Online.pdf.

89 Hitt et al., *The Business of Voting*, 9–27.

90 Secure Elections Act, S. 2261, 115th Cong. (2017); in a similar vein, the Election Vendor Security Act, H.R. 6435, 115th Cong. (2018), requires vendors to "report any known or suspected security incidents involving election systems . . . not later than 10 days after the vendor first knows or suspects that the incident occurred."

91 Matthew Cole et al., "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election," *Intercept*, Jan. 5, 2017, https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election.

92 United States v. Netyksho et al., No. 1:18CR00215, 2018 WL 3407381, at 26 (D.D.C. Jul. 13, 2018).

93 VR Systems, Letter to Sen. Ron Wyden, May 16, 2019, https://www.politico.com/f/?id=0000016a-e72c-d72a-af6e-f72eb6550002. According to the letter, EViD "is a front-end system used to check voters in at the polls and to provide information such as a voter's polling location when they search for it."

94 Liberty Systems, LLC, "About Us," http://libertysystemsllc.com/.

95 Undersecretary of Defense, *Memorandum Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review, U.S. Department of Defense*, Jan. 21, 2019, https://www.acq.osd.mil/dpap/pdi/cyber/docs/USA000140-19%20TAB%20A%20USD(AS)%20Signed%20Memo.pdf.

96 U.S. Election Assistance Commission, *Testing and Certification Program Manual, Version 2.0*, 71.

97 U.S. Election Assistance Commission, *Testing and Certification Program Manual, Version 2.0*, 73.

98 Securing America's Federal Elections Act, H.R. 2722, 116th Cong. (2019), § 202; For the People Act, H.R. 1, 116th Cong. (2019), § 3301.

99 Protect Election Systems from Foreign Control Act, H.R. 6449, 115th Cong. (2018), § 304.

100 U.S. Department of Defense, "Department of Defense Expands 'Hack the Pentagon' Crowdsourced Digital Defense Program," Oct. 24, 2018, https://dod.defense.gov/News/News-Releases/News-Release-View/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr.

101 For the People Act, H.R. 1, 116th Cong. (2019), § 3402.

102 *A Framework for a Vulnerability Disclosure Program for Online Systems, Version 1.0*, Cybersecurity Unit, Computer Crime & Intellectual Property Section, Criminal Division, U.S. Department of Justice, July 2017, https://www.justice.gov/criminal-ccips/page/file/983996/download.

103 Defense Contract Management Agency, "About the Agency," https://www.dcma.mil/About-Us/.

104 Defense Contract Management Agency, "About the Agency."

105 See generally, Defense Contract Management Agency, "What DCMA Does," Aug. 22, 2016, https://www.dcma.mil/News/Videos/videoid/480264/nav/Default/.

106 10 C.F.R. §§ 19.1–19.40.

107 10 C.F.R. § 19.14(a).

108 10 C.F.R. §§ 73.1–73.81.

109 U.S. Election Assistance Commission, *Testing and Certification Program Manual, Version 2.0*, 65.

110 U.S. Election Assistance Commission, *Testing and Certification Program Manual, Version 2.0*, 69.

111 Thomas R. Wilkey (executive director, U.S. Election Assistance Commission), letter to Steve Pearson (vice president, Election Systems & Software), July 21, 2009, https://www.eac.gov/voting-equipment/-unity-3200.

112 Brian J. Hancock (director, Testing & Certification Program, U.S. Election Assistance Commission), letter to Steve Pearson (vice president, Election Systems & Software), Mar. 1, 2011, https://www.eac.gov/voting-equipment/-unity-3200.

113 Mark Robbins (general counsel and acting executive director, U.S. Election Assistance Commission), letter to Steve Pearson (vice president, Election Systems & Software), Feb. 1, 2012, https://www.eac.gov/voting-equipment/-unity-3200.

114 Steve Pearson (vice president, Election Systems & Software), letter to Mark Robbins (general counsel and acting executive director, U.S. Election Assistance Commission), Feb. 7, 2012, https://www.eac.gov/voting-equipment/-unity-3200.

115 Kathy Rogers (vice president, Election Systems & Software), letter to Brian J. Hancock (director, Testing & Certification Program, U.S. Election Assistance Commission), Aug. 3, 2012, https://www.eac.gov/voting-equipment/-unity-3200.

Endnotes for Sidebar

i U.S. Election Assistance Commission, *Testing and Certification Program Manual, Version 2.0*, 12–19.

ii *Voluntary Voting Systems Guidelines, Vol.1, Version 1.1*, §7.4.6, §7.5, §7.5.2, §7.5.3.

iii The adoption of modern approaches such as agile software development and the provision of ongoing technical support makes information about a vendor's ongoing compliance with best practices critical for determining the level of risk posed by upgrades and changes, including some that might be deemed de minimis if vendor security practices are strong. See U.S. Election Assistance Commission, *Testing and Certification Program Manual, Version 2.0*.

iv U.S. Election Assistance Commission, *Testing and Certification Program Manual, Version 2.0*, 17. Suspension of an entire vendor, like decertification of a vendor, would similarly need to be handled thoughtfully. See Enforcing Guidelines section on this report.

Image Credits:

Page 5: REVA/Noun Project, Pravin Unagar/Noun Project, Aisyah/

ABOUT THE AUTHORS

▶ **Lawrence Norden** is director of the Election Reform Program at the Brennan Center for Justice, where he leads efforts to bring balance to campaign funding and break down barriers that keep Americans from participating in politics, ensure that U.S. election infrastructure is secure and accessible to every voter, and protect elections from foreign interference. He has authored several nationally recognized reports and articles related to voting rights and voting technology, including *Securing Elections From Foreign Interference* (2017), *America's Voting Machines at Risk* (2015), and *How to Fix Long Lines* (2013). His work has been featured in media outlets across the country, including the *New York Times*, the *Wall Street Journal*, Fox News, CNN, MSNBC, and National Public Radio. He has testified before Congress and several state legislatures on numerous occasions. Norden is a member of the Election Assistance Commission's Board of Advisors. This report is not affiliated with his role as an EAC advisor. He is a graduate of the University of Chicago and NYU School of Law.

▶ **Christopher R. Deluzio** is the policy director of the University of Pittsburgh's Institute for Cyber Law, Policy, and Security. He was previously counsel in the Democracy Program at the Brennan Center for Justice, where his writing included nationally recognized work on voter purges, a procurement guide to assist in the selection and management of election vendors, and legal analysis of speech restrictions in polling places. Prior to joining the Brennan Center, he was a litigation associate in private practice with Wachtell, Lipton, Rosen & Katz and, before that, law clerk to Judge Richard J. Sullivan of the U.S. District Court for the Southern District of New York. He graduated magna cum laude from Georgetown Law, where he was elected to the Order of the Coif, served as an executive articles editor of the *Georgetown Law Journal*, and was selected as the top oralist in the Robert J. Beaudry Moot Court Competition and the Thurgood A. Marshall Memorial Moot Court Competition. He received a bachelor's degree from the U.S. Naval Academy and, following graduation, served as an active-duty naval officer.

▶ **Gowri Ramachandran** is senior counsel in the Brennan Center for Justice's Democracy Program. She comes to the Brennan Center from Southwestern Law School in Los Angeles, California, where she is on leave from her position as professor of law. At Southwestern, she taught courses in constitutional law, employment discrimination, and critical race theory, as well as the Ninth Circuit Appellate Litigation Clinic, which received the Ninth Circuit's 2018 Distinguished Pro Bono Service Award. She received her undergraduate degree in mathematics from Yale College and a master's degree in statistics and JD from Harvard University. While in law school, she served as editor in chief of the *Yale Law Journal*. After graduating from law school in 2003, Ramachandran served as law clerk to Judge Sidney R. Thomas of the U.S. Court of Appeals for the Ninth Circuit in Billings, Montana. After a fellowship at Georgetown Law, she joined the Southwestern faculty in 2006.

ACKNOWLEDGMENTS

The Brennan Center gratefully acknowledges BLT Charitable Trust, Carnegie Corporation of New York, Craig Newmark Philanthropies, Ford Foundation, Lee Halprin and Abby Rockefeller, The JPB Foundation, Leon Levy Foundation, Open Society Foundations, Barbara B. Simons, Wallace Global Fund, and Leslie Williams for their generous support of our election security work.

The authors would like to thank the numerous Brennan Center colleagues who collaborated in preparing this report. Brennan Center Fellow Derek Tisler and Legal Intern Cara Ortiz contributed crucial research and editorial support. Edgardo Cortés, Elizabeth Howard, and Daniel I. Weiner provided helpful revisions. Jeanne Park and Matthew Harwood of the Brennan Center's communications team lent valuable review and editing assistance. The authors are grateful to Research and Program Associate Andrea Córdova McCadney for assistance in citation-checking and editing. The editorial and design assistance of Alexandra Ringe, Alden Wallace, Rebecca Autrey, and Zachary Laub allowed this report to reach publication.

This report also benefited from the many people willing to share their valuable expertise and provide insight in the review process. We gratefully acknowledge the following individuals for their helpful feedback: Marian Schneider, president, Verified Voting; Ryan Macias, election technology and security expert; Susan Greenhalgh, vice president for programs, National Election Defense Coalition; Bruce Schneier, security technologist and adjunct lecturer in public policy, Harvard Kennedy School; Gregory A. Miller, cofounder and chief operating officer, OSET Institute; E. John Sebes, cofounder and chief technology officer, OSET Institute; and Eddie Perez, global director of technology R&D, OSET Institute.

BRENNAN
CENTER
FOR JUSTICE

Brennan Center for Justice at New York University School of Law
120 Broadway // 17th Floor // New York, NY 10271
www.brennancenter.org

Appendix B

POLICY REPORT

BRENNAN
CENTER
FOR JUSTICE

Preparing for Cyberattacks and Technical Failures

A Guide for Election Officials

By Edgardo Cortés, Gowri Ramachandran, Liz Howard, and Lawrence Norden

PUBLISHED DECEMBER 19, 2019

Brennan Center for Justice at New York University School of Law

Table of Contents

STAY CONNECTED TO THE BRENNAN CENTER

Visit our website at
www.brennancenter.org

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that works to reform, revitalize — and when necessary defend — our country's systems of democracy and justice. The Brennan Center is dedicated to protecting the rule of law and the values of constitutional democracy. We focus on voting rights, campaign finance reform, ending mass incarceration, and preserving our liberties while also maintaining our national security. Part think tank, part advocacy group, part cutting-edge communications hub, we start with rigorous research. We craft innovative policies. And we fight for them — in Congress and the states, in the courts, and in the court of public opinion.

ABOUT THE BRENNAN CENTER'S DEMOCRACY PROGRAM

The Brennan Center's Democracy Program works to repair the broken systems of American democracy. We encourage broad citizen participation by promoting voting and campaign finance reform. We work to secure fair courts and to advance a First Amendment jurisprudence that puts the rights of citizens — not special interests — at the center of our democracy. We collaborate with grassroots groups, advocacy organizations, and government officials to eliminate the obstacles to an effective democracy.

Introduction

America's intelligence agencies have unanimously concluded that the risk of cyberattacks on election infrastructure is clear and present — and likely to grow.[1] While officials have long strengthened election security by creating resiliency plans,[2] the evolving nature of cyber threats makes it critical that they constantly work to improve their preparedness. It is not possible to build an election system that is 100 percent secure against technology failures and cyberattacks, but effective resiliency plans nonetheless ensure that eligible voters are able to exercise their right to vote and have their votes accurately counted. This document seeks to assist officials as they revise and expand their plans to counter cybersecurity risks.

Many state and local election jurisdictions are implementing paper-based voting equipment, risk-limiting audits, and other crucial preventive measures to improve overall election security. In the months remaining before the election, it is at least as important to ensure that adequate preparations are made to enable quick and effective recovery from an attack if prevention efforts are unsuccessful.

While existing plans often focus on how to respond to physical or structural failures, these recommendations spotlight how to prevent and recover from technological errors, failures, and attacks. Advocates and policymakers working to ensure that election offices are prepared to manage technology issues should review these steps and discuss them with local and state election officials.

Prevent and Recover from Electronic Pollbook Failures and Outages

Electronic pollbooks, or e-pollbooks, are laptops or tablets that poll workers use instead of paper lists to look up voters. E-pollbooks expedite the administration process, shorten lines, lower staffing needs, and save money. Most e-pollbooks can communicate with other units in the same location to share real-time voter check-in updates. They may also be able to communicate directly with a local election office or with other locations, such as vote centers, via physical connections or wireless networks.

There are no national standards for e-pollbook operations or security. E-pollbooks present unique challenges because they need to maintain updated information across numerous devices and locations. Additionally, many devices that may be used as e-pollbooks do not have the ability to connect via physical networks and require some type of wireless communication to convey important information. Election officials should consider the following security recommendations when using e-pollbooks:

Limit or eliminate connectivity to wireless networks whenever possible. E-pollbooks used for voter check-in generally do not need wireless connections. Officials who operate precinct-based voting on Election Day should choose e-pollbook options that use hardwired connections to share voter information in real time across units to complete the voter check-in process. This provides the greatest level of security. Bluetooth is not an acceptable alternative to other types of wireless network connectivity; researchers have found security vulnerabilities that risk the spread of malware and allow unauthorized access to data being transmitted between Bluetooth-connected devices.[3]

Implement proper security protocols when wireless connectivity is required. Election officials using vote centers and multiple early-voting locations may require some network connectivity to share voter check-in information across several locations. Additionally, some e-pollbooks may not fully function if their wireless connections are eliminated or disabled. For example, certain e-pollbooks use Apple iPads, which rely solely on wireless connectivity for communication. If wireless networks must be used, officials should implement security protocols, including encrypting communication between e-pollbooks and requiring strong passwords that are changed after every election.

Ensure that systems are properly patched as part of Election Day preparations. E-pollbooks must receive appropriate operating system updates and software patches in advance of every election to protect against known cyber vulnerabilities. To determine what patches are available or recommended, election officials should start by reviewing any guidelines or requirements created by state or local government IT agencies. States and localities may develop their cybersecurity requirements on the basis of the National Institute of Standards and Technology's cybersecurity framework.[4] Adhering to these requirements will ensure that election officials are using best practices for securing election systems, protecting the personally identifiable information (PII) of voters, and preserving the integrity of voter data used on Election Day. Alerts from the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) can also provide insights about recent vulnerabilities and emergency security patches.

Keep appropriate backup of e-pollbooks in polling places. Paper backups of e-pollbooks are the best resiliency measure in the event of an e-pollbook failure. They allow poll workers to continue confirming voters' eligibility, diminish the potential for long lines, and may minimize the need to issue provisional ballots. While jurisdictions in 41 states and the District of Columbia (DC) use e-pollbooks, our research indicates that only 11 states and DC formally require paper backups on Election Day, although several other states recommend the practice or have counties that voluntarily keep paper backups.[5] Durham County, North Carolina, experienced a significant failure of e-pollbooks in November 2016, when many voters arrived at the polls to find that they had been marked on the e-pollbooks as already having voted or were improperly marked as needing to provide additional identification.[6] Voting was delayed for more than an hour and a half as the county printed paper pollbooks and delivered them.[7] This delay could have been avoided if printed pollbooks had been sent ahead of time with other polling place materials. Preemptively sending paper backup of e-pollbooks to polling places obviates the need for detailed logistics in case of e-pollbook failure.

Jurisdictions should evaluate their e-pollbook recovery procedures to ensure they will be easy for poll workers to follow and will not introduce new obstacles to voters casting their ballots quickly. As the use of vote centers and other centralized voting locations increases, printing pollbooks may create logistical and administrative challenges. These types of voting locations may need other backup options, such as nonnetworked devices from a different vendor that contain the entire list of registered voters for a jurisdiction, along with the correct ballot style and current status (i.e., voted, absentee, or not voted) for each voter. Another option is to produce a backup list on demand using high-speed printers. This backup procedure, which New Hampshire law calls for, could allow polling places to quickly transition from malfunctioning e-pollbooks to paper backups.

Provide sufficient provisional ballots and materials for two to three hours of peak voting. A key backup measure for Election Day is to supply sufficient provisional ballots and provisional balloting materials. It is preferable to issue regular ballots to eligible voters if the e-pollbook system fails. However, it may not be possible to determine voter eligibility in the event of such a failure, especially if backup paper pollbooks are unavailable or are found to contain errors. Provisional ballots ensure that individuals can cast a ballot while providing election officials time to determine their eligibility. These ballots should be counted once officials determine eligibility, with no further action required of the voter. Having sufficient provisional ballots to account for two to three hours of peak voting activity will allow voting to continue in the event of system failures.[8] For the November 2020 election, this will require enough provisional ballots for at least 35 percent of registered voters.[9] While not enough to deal with an all-day problem, it will provide sufficient time for other measures to be implemented or additional ballots and materials to be delivered. Contingency plans must provide for additional materials to be delivered if the problem cannot be resolved.

Train poll workers to implement pollbook contingencies. Improper or insufficient training of poll workers can lead to voters being turned away, long lines, and ineligible individuals casting ballots. Poll worker instructions for managing provisional ballots must specify how to handle e-pollbook failures appropriately, including when to allow voters to cast a regular ballot and when to issue provisional ballots instead. Whenever voter eligibility can be confirmed in a timely fashion through the use of appropriate backups, regular ballots should be issued. The U.S. Election Assistance Commission (EAC) provides a list of guidelines for poll workers regarding provisional ballots as well as some best practices for poll worker accountability. Provisional ballot forms must clearly indicate the sections that should be filled out by voters, poll workers, and election staff, so each person knows what he or she needs to do. It is also important to provide a clear list of circumstances in which to use provisional ballot envelopes, including on the envelopes themselves. In 2018, Virginia adopted new provisional ballot materials created in coordination with the Center for Civic Design that illustrate these best practices.[10]

More Resources

Center for Internet Security Handbook
www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf

Belfer Center Cybersecurity Playbook
www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook#voterreg

Pew E-pollbook Database
www.pewtrusts.org/en/research-and-analysis/data-visualizations/2017/a-look-at-how-and-how-many-states-adopt-electronic-poll-books

National Conference of State Legislatures Page on E-pollbooks
www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx

EAC Standards for Poll Workers
www.eac.gov/research-and-data/provisional-voting

Center for Civic Design on Provisional Ballots
www.civicdesign.org/you-see-a-provisional-ballot-voters-see-their-ballot

Prevent and Recover from Voting Equipment Failures

Even under the best of circumstances, equipment failures occur. For digital or optical-scan voting systems, recovery in case of an equipment failure can be relatively fast; as ballots are already printed, voting can continue while the tabulator issue is resolved. As a Brennan Center report on voting machines notes, jurisdictions that rely on direct-recording electronic (DRE) machines can face more problems in the event of a failure, since "voters may have to wait in long lines while election workers scramble to repair them."[11]

These problems can occur when jurisdictions use ballot-marking devices (BMDs) and ballot-on-demand (BOD) printers as well. In the event of a system failure, these machines will not function until repaired or replaced, and jurisdictions using them will need to print ballots in advance of the election to allow voting to continue. Regardless of the voting system used, election officials should conduct logic and accuracy testing on all voting equipment prior to every election in order to minimize the chance of unforeseen failures on Election Day.

If using paper ballots, print enough ballots for all registered voters. Many election officials using paper ballots decide how many ballots to print on the basis of prior election turnout or the percentage of registered voters expected to vote. This approach can result in ballot shortages and leave jurisdictions unprepared for unexpected voter surges. This happened across the country during the 2018 midterm elections, when turnout reached historic levels, and many experts predict record-breaking turnout in 2020.[12] To prepare, election officials should print enough ballots for all registered voters. Jurisdictions that allow Election Day registration may require an even higher ballot supply.

If using voting systems that do not require preprinted ballots, print enough emergency paper ballots for two to three hours of peak voting activity. Emergency ballots should be provided to voters who are identified as qualified and meeting all the requirements for voting pursuant to state law but who are unable to vote due to a voting machine malfunction. Emergency ballots are different from provisional ballots, which are given to voters whose eligibility is unclear. Emergency ballots should be counted as soon as functional voting equipment becomes available, without any additional scrutiny of voter qualifications, unlike provisional ballots, which may require research on voter eligibility. Printing enough emergency ballots for two to three hours of peak voting activity will allow voting to continue until equipment can be repaired or replaced, or until additional paper ballots can be delivered to a polling place. For the November 2020 election, this will require enough provisional ballots for at least 35 percent of registered voters. Appropriate procedures should be put in place for chain of custody and accounting for preprinted paper ballots.

DRE voting systems directly record, in electronic form, voters' selections in each race or contest on the ballot. An increasing number of states and local jurisdictions have begun replacing antiquated DREs with BMDs as the primary voting option. Others are increasingly using vote centers, which often rely on BOD printers to produce on-site any ballot style and language that might be needed for a particular voter. Because these systems do not need preprinted ballots, election jurisdictions using DREs, BMDs, or BOD-printed ballots as their primary voting option should preprint and distribute emergency paper ballots that can be counted by existing tabulators. There are 16 states that will use DREs as the principal polling place equipment in at least some jurisdictions in 2020.[13] However, at least seven do not mandate that paper ballots be made available in the event of DRE failure.[14]

In vote centers that have a large number of ballot styles, preprinted emergency ballots for at least the precincts closest to that vote center should be stocked. Vote centers can also be stocked with master copies of emergency paper ballots in all necessary styles and languages, along with a photocopier to reproduce them in emergency situations.

Tabulators should be programmed to accept and read both ballots produced by the BMD/BOD printers and preprinted emergency ballots. Preelection testing should verify that the tabulators properly identify and record both types of ballots.

Develop procedures to manage and track malfunctioning equipment or equipment failure. Machines that appear to be malfunctioning or improperly calibrated should be taken out of service and additional voting equipment deployed to the polling place or vote center. Recalibrating DRE touch screens or conducting any other necessary voting equipment repairs should be done in full view of observers. Any reports from voters of machine errors should be tracked and immediately reported to the central election office. Election offices should review and compare these reports across voting locations to identify trends that could indicate widespread problems, including potential cyberattacks. Training should ensure that poll workers understand the process for counting ballots, including potentially hand-counting ballots, if equipment failure cannot be resolved before voting ends.

Communicate with voters to build trust in the election process. Election officials should preprint signage that will allow poll workers to inform voters of equipment failures in a manner that is consistent across locations and approved by the election office. On Election Day, poll workers should ensure that voters are not directed to use machines that are suspected of producing erroneous records.

Poll workers should also take steps to make sure that voters accurately recorded their selections on their ballots. When using hand-marked paper ballots that are counted without the help of an optical scanner, poll workers should remind voters to check their ballots to prevent overvotes, which occur when voters make more selections than the number allowed. When using DREs with a voter-verifiable paper audit trail (VVPAT) or BMDs, poll workers should clearly explain to voters how their ballots will be cast and remind them to verify that the paper printout matches the selections they made on the machine. For example, when using BMDs that print a ballot that must then be scanned by a separate machine, poll workers should say to voters, after their ballot has been printed and before it is cast: "Don't forget to check the printed ballot carefully. If you see something wrong, you can get a replacement. Then you'll go [over there] to cast it."

Take steps to prevent late polling place openings due to equipment failures. Inoperable voting equipment should not prevent the timely opening of a polling place. Late polling place openings can lead to long lines and voters leaving without an opportunity to cast a ballot.[15] Poll workers should be trained to deal with equipment failures occurring on the morning of Election Day. Voters should be allowed to vote using emergency paper ballots if voting equipment is not operable when the polls open. Poll workers should explain to voters how their ballots will be counted once working voting equipment becomes available.

Plan to assist voters with disabilities if voting machines fail. If accessible voting machines fail and paper ballots are used instead, disabled voters may not be able to vote privately and independently. Jurisdictions with sufficient resources should have backup accessible voting equipment, with all ballot styles available (similar to what would be used at a central voting site for early voting), geographically dispersed so that it can be rapidly delivered to any polling place where accessible equipment has failed. In the longer term, jurisdictions might consider providing each polling place with accessible tablets and printers to be used by voters with disabilities in the event of equipment failure.[16] Poll workers should be appropriately trained on any backup systems used to provide accessibility.

More Resources

Brennan Center Report on Voting Machines at Risk
www.brennancenter.org/analysis/americas-voting-machines-risk-an-update

Brennan Center Voting Equipment Overview
www.brennancenter.org/analysis/overview-voting- equipment

Verified Voting Verifier – Lookup Tool for Polling Place Equipment
www.verifiedvoting.org/verifier

Prevent and Recover from Voter Registration System Failures and Outages

Voter registration systems maintain official lists of registered voters, including all voter information and district assignment information. The statewide systems usually serve additional election-management purposes as well, such as processing absentee ballots. A failure of the registration system on or near Election Day can cause problems producing files for paper pollbooks or e-pollbooks, using voter information lookup tools, or validating provisional ballots immediately after the election.

Establish a 60-day preelection blackout window for all noncritical software updates and patches. These windows increase the likelihood that programming errors, viruses, or other problems will be discovered in a timely manner prior to Election Day. Sixty days provides sufficient time before the close of voter registration or the start of absentee voting to identify whether installed patches or updates have created unintended system issues. Even updates that do not directly impact voter registration databases, such as server patching, networking equipment upgrades, and locality telecommunications system changes, may impact a local election official's ability to access the state voter registration database. Therefore it is critical that these blackout dates be established and communicated with relevant staff to prevent potential issues on or shortly before Election Day. The plan should include a process for emergency updates during the blackout window, indicating who will authorize the emergency update and how it will be tested prior to rollout.

Subject the system periodically to independent vulnerability testing. States can either partner with the Department of Homeland Security or engage outside cybersecurity consultants to test the system for vulnerabilities on a periodic basis. Vulnerability testing should be conducted well in advance of an election, and at least quarterly, to provide sufficient time to resolve any potential vulnerabilities that are discovered. While the specific results of vulnerability testing need not be released so as to maintain system security, officials should be transparent about what entity conducted the testing and what standards it used.

Maintain backup copies of digital records off-line in case online access is limited. In the lead-up to the election, local officials should download an electronic copy of voter information on a daily basis and store it securely, so that they have the most recent information in case the voter registration system becomes unavailable. This can be used to conduct research on provisional ballots after the election.

Provide voters with tools to look up their voter registration status online and conduct outreach to urge voters to use the tool in advance of any registration deadline. Voters can provide crucial information about undesired changes to their registration, including address changes they did not request, which could be an early indicator of a possible breach. Encouraging voters to check before a deadline ensures that problems can be resolved in a timely fashion. It may also reduce pressure on poll workers on Election Day.

Provide voters with tools to look up their polling place information online, and make alternative websites available. In case a voter lookup tool fails, election officials should be prepared to provide links to other polling place lookup tools, such as the Voting Information Project (VIP), an independent entity that provides information to voters using official data. New Jersey successfully used VIP to provide information to voters after Hurricane Sandy made state systems unavailable and necessitated a large number of polling place changes in advance of the 2012 election.[17] Using tools such as VIP for polling place lookups, instead of sites that depend on statewide registration systems, also reduces the load on state servers at busy times in the election season. This requires providing accurate polling place data to the backup site in advance of elections and confirming that the backup site is working correctly.

More Resources

EAC Deep Dive on Election Technology
www.eac.gov/documents/2018/05/01/eavs-deep-dive-election-technology

Pew Project on Upgrading Voter Registration
www.pewtrusts.org/en/projects/election-initiatives/about/upgrading-voter-registration

EAC Checklist for Securing Voter Registration Data
www.eac.gov/documents/2017/10/23/checklist-for-securing-voter-registration-data

Voting Information Project
www.votinginfoproject.org

Prevent and Recover from Election Night Reporting System Failures and Outages

Local and state officials usually post unofficial results on election night. While this information does not reflect the certified results, large differences between unofficial election night results and the final outcome can create questions for voters about the accuracy of the process. Election night reporting sites are prime targets for denial of service (DoS) attacks because the sites' high-use period is known ahead of time, and preventing access to unofficial results can create negative media attention about the electoral process. A hotly contested race can intensify interest in the election results, and a large increase in visitors to a reporting site in a short period can likewise bring down the site.

Establish redundancies. Some states, including Arizona and Virginia, experienced election night reporting failures in the 2014 midterm elections.[18] Addressing the system failures after the election, several of these states established a redundant system that can be made available if the main system fails.[19]

Do not connect election night reporting systems to voting systems or the statewide registration system. Election night reporting systems (ENRs) are attractive targets for cybercriminals and other nations. Bad actors have successfully attacked ENRs around the world, including in Ukraine, Bulgaria, and more recently the United States. By publishing unofficial results through an unconnected system, election officials can minimize the potential that a targeted attack on the reporting system will have any lasting impact. Knox County, Tennessee, experienced a DoS attack linked to foreign IP addresses during its May 1, 2018, primary elections. Although this attack likely served as a distraction from a separate attack on the county's servers, the reporting website itself did not provide an avenue for future disruption. The county's deputy director of IT noted that its reporting system is "not connected to any live databases. . . . It's a repository for being able to report to the public, and we have intentionally kept any primary data extremely isolated."[20]

More Resources

EAC Checklist for Securing Election Night Reporting Systems
www.eac.gov/documents/2017/10/23/checklist-for-securing-election-night-reporting-systems-data- election-administration-security

Communication Strategy

All good contingency plans include a communication plan. At its core, a communication plan is intended to assist election officials in distributing essential information in a timely manner and maintaining public confidence in the election's administration. Communication plans are important in all unexpected situations, from equipment failures to potential cyberattacks to unintentional errors.

Draft, review, and approve a communication plan prior to Election Day. Keeping voters, poll workers, and others informed minimizes the harm that could arise on Election Day in the event of negative developments. The most basic communication plan includes key staff and contacts. A more detailed strategy may include various response options for potential problems as well as longer-term considerations, such as notification requirements in the event personal voter information has been leaked.

Provide a public website for emergency communications. Officials should publicize links where emergency information will be posted on Election Day, possibly including official social media accounts used by state and local election officials. These can serve as official sources where voters, candidates, media, and advocacy organizations can find information regarding extended polling place hours, polling place relocations, and other emergency information. Doing this in advance of an election will make emergency communications easier for election officials.

Be transparent but careful. As the Belfer Center for Science and International Affairs suggests, "Transparent communication builds trust, but in a cyber incident, you will have few facts at hand, especially at the outset. Public comments should demonstrate that you are taking the issue seriously but avoid providing any details that may change as the investigation progresses, so you don't have to correct yourself down the line. Avoid speculation on the perpetrator of the incident."[21]

More Resources

Belfer Center Cybersecurity Playbook
www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook#voterreg

Endnotes

[1] See generally Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1*, 2019, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf; 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; and Olivia Gazis, "Intel Chiefs Warn of Russia-China Alliance as Threats Grow More Complex," CBS News, Jan. 29, 2019, https://www.cbsnews.com/news/intelligence-chiefs-provide-updates-on-worldwide-threats-2019-01-28-live-updates.

[2] See, e.g., Wisconsin State Board of Elections, *Report on Election Related Contingency Planning*, 2007, https://elections.wi.gov/sites/default/files/publication/65/election_related_contingency_planning_2007_pdf_19060.pdf; Senate Select Committee on Intelligence, *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Draft SSCI Recommendations*, 2018, https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings%2CRecs2.pdf.

[3] See, e.g., Armis, *Protecting the Enterprise from BlueBorne*, 2017, https://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper.pdf; Daniele Antonioli, Nils Ole Tippenhauer, and Kasper B. Rasmussen, "The KNOB Is Broken: Exploiting Low Entropy in the Encryption Key Negotiation of Bluetooth BR/EDR" (paper presented at the 28th Usenix Security Symposium, Santa Clara, CA, Aug. 2019), https://www.usenix.org/conference/usenixsecurity19/presentation/antonioli.

[4] National Institute of Standards and Technology, "Cybersecurity Framework," accessed Nov. 20, 2019, https://www.nist.gov/cyberframework.

[5] In our research, we found written paper backup requirements for e-pollbooks in 11 states and Washington, DC. These 11 states are Connecticut, Georgia, Michigan, Minnesota, New Jersey, North Carolina, Ohio, Pennsylvania, Rhode Island, South Carolina, and South Dakota. Mississippi and West Virginia have laws recommending paper backups. In Nevada and Wyoming, backup paper pollbooks are available in practice everywhere e-pollbooks are used, while in other states, like Colorado, Kansas, and Texas, paper backups are available in many jurisdictions. Arizona and Maryland formally require that either paper or electronic backups be available, while Idaho has indicated that it makes this recommendation. A few other states require or recommend that electronic backups be available. New Hampshire mandates that a sufficient number of high-speed printers be available to produce a backup paper checklist in the event of a system failure but has not yet deployed its e-pollbook solution.

[6] Pam Fessler, "Russian Cyberattack Targeted Elections Vendor Tied to Voting Day Disruptions," NPR, Aug. 10, 2018, https://www.npr.org/2017/08/10/542634370/russian-cyberattack-targeted-elections-vendor-tied-to-voting-day-disruptions.

[7] Fessler, "Russian Cyberattack Targeted Elections Vendor."

[8] Nicholas Weaver, "Election Vulnerability: Voter Registration Systems," *Lawfare*, Feb. 23, 2018, https://www.lawfareblog.com/2018-election-vulnerability-voter-registration-systems.

[9] In the typical state, 35 to 45 percent of voters surveyed arrived at their polling place during the peak three hours of voting. Because historically high turnout is expected in the 2020 elections, we multiplied this range by 90 percent, to estimate that emergency supplies to serve 30 to 40 percent of voters would be prudent, or 35 percent in the typical case. See Charles Stewart III, *2016 Survey of the Performance of American Elections: Final Report*, Massachusetts Institute of Technology, 2017, 343, http://www.legendsvote.org/wp-content/uploads/MIT-Charles-Stewart-Voter-Turnout-Study-2016.pdf.

[10] Center for Civic Design, "Making Provisional Voting Easier in Virginia," accessed Nov. 20, 2019, https://civicdesign.org/showcase/making-provisional-voting-easier-in-virginia.

[11] Lawrence Norden and Christopher Famighetti, *America's Voting Machines At Risk*, Brennan Center for Justice, 2015, 30, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.

[12] Henry Olsen, "We Could Have Record Turnout in the 2020 Election. We're Not Ready for It," *Washington Post*, Oct. 10, 2019, https://www.washingtonpost.com/opinions/2019/10/10/we-could-have-record-turnout-election-were-not-ready-it.

[13] These 16 states are Arkansas, Indiana, Illinois, Kansas, Kentucky, Louisiana, Mississippi, Nevada, New Jersey, North Carolina, Ohio, Texas, Tennessee, Utah, Wyoming, and West Virginia. Three states that have recently used DREs — Georgia, South Carolina, and Pennsylvania — have committed to replacing them by 2020.

[14] We have identified the following states where there are no provisions mandating that paper ballots be made available in the event of DRE failure: Kansas, Nevada, North Carolina, Texas, Utah, West Virginia, and Wyoming. While not required by statute, polling places in some of these states may provide some form of emergency paper ballots when systems go down. For instance, Kansas requires counties to keep an additional supply of ballots to meet any emergency need for such ballots, although machine failure is not specifically listed; Nevada requires each local election official to submit a plan for the use of absentee ballots in case of an emergency; Texas advises its counties to adopt procedures to provide emergency paper ballots in the event of DRE machine failure; Utah allows the provision of emergency paper ballots; and West Virginia counties have contingency plans in the event of machine failure.

[15] For example, during New York's June 2018 federal primary election, a voter was reportedly unable to vote because an election worker had not yet activated voting equipment. The voter was not offered an emergency ballot before having to leave the polling place. See Jake Offenhartz, "Voters Reporting Closed Poll Sites and Other Primary Day Confusion," *Gothamist*, June 26, 2018, http://gothamist.com/2018/06/26/voters_primary_confusion_nyc.php.

[16] States like Oregon have adopted remote accessible voting by mail without requiring access to the internet to mark the ballot. Jurisdictions may want to consider having such systems available in the polling place in the event of machine failures. See State of Oregon, "Voting Instructions for Voters with a Disability," accessed Nov. 20, 2019, https://sos.oregon.gov/voting/Pages/instructions-disabilities.aspx.

[17] Susan K. Urahn, "Collaboration, Technology and the Lessons of Election Day," *Governing: States and Localities*, Jan. 16, 2013, https://www.governing.com/columns/mgmt-insights/col-collaboration-technology-voting-information-accessibility.html.

[18] Eyragon Eidam, "Is Your Election Night Reporting System Ready for 2016?"*Government Technology*, Dec. 21, 2015, http://www.govtech.com/state/Is-Your-Election-Night-Reporting-System-Ready-for-2016.html.

[19] Eidam, "Is Your Election Night Reporting System Ready?"

[20] Sam Levine, "Hackers Tried to Breach a Tennessee County Server on Election Night: Report," *Huffington Post*, May 11, 2018, https://www.huffpost.com/entry/knox-county-election-cyberattack_n_5af5ca21e4b032b10bfa56ee; and Tyler Whetstone, "Knox County Election Night Cyberattack Was Smokescreen for Another Attack," *Knox News*, May 17, 2018, https://www.knoxnews.com/story/news/local/2018/05/17/knox-county-election-cyberattack-smokescreen-another-attack/620921002/.

[21] Siobhan Gorman et al., *Election Cyber Incident Communications Coordination Guide*, Belfer Center for Science and International Affairs, 2018, 12, https://www.belfercenter.org/sites/default/files/files/publication/CommunicationsGuide.pdf.

ABOUT THE AUTHORS

▶ **Edgardo Cortés** is the election security adviser for the Brennan Center's Democracy Program. An expert on election administration and policy, Cortés served as Virginia's first commissioner of elections. During his tenure, he served as chairman of the board for the Election Registration Information Center and chairman of the U.S. Election Assistance Commission Standards Board. He previously served as the general registrar in Fairfax County, Virginia, and deputy director for policy and grants director at the U.S. Election Assistance Commission. Cortés received his undergraduate degree from Cornell University and his master's degree in political management from George Washington University.

▶ **Gowri Ramachandran** serves as counsel for the Brennan Center's Democracy Program. She came to the Brennan Center from Southwestern Law School in Los Angeles, where she is on leave from her position as professor of law. At Southwestern, she has taught courses in constitutional law, employment discrimination, and critical race theory, as well as the Ninth Circuit Appellate Litigation Clinic, which received the Ninth Circuit's 2018 Distinguished Pro Bono Service Award. She received her JD from Yale Law School.

▶ **Liz Howard** serves as counsel for the Brennan Center's Democracy Program, where she works on cybersecurity and elections. Prior to joining the Brennan Center, Howard served as deputy commissioner of the Virginia Department of Elections. During her tenure, she coordinated many election administration modernization projects, including the decertification of all paperless voting systems, implementation of the e-Motor Voter program, and adoption of online, paperless absentee ballot applications. Before her appointment, she worked as general counsel at Rock the Vote and as a senior associate at Sandler Reiff. She received her JD from William and Mary School of Law.

▶ **Lawrence Norden** is director of the Brennan Center's Election Reform Program. He has authored several nationally recognized reports and articles related to voting rights and voting technology, including *Securing Elections from Foreign Interference* (2017), *America's Voting Machines at Risk* (2015), *How to Fix Long Lines* (2013), *Better Design, Better Elections* (2012), and *Voting Law Changes in 2012* (2011). His work has been featured in media outlets across the country, including the *New York Times,* the *Wall Street Journal*, CNN, Fox News, MSNBC, and NPR. He has testified before Congress and several state legislatures on numerous occasions. He received his JD from New York University School of Law.

ACKNOWLEDGMENTS

The Brennan Center gratefully acknowledges Carnegie Corporation of New York, Change Happens Foundation, Craig Newmark Philanthropies, Lee Halprin and Abby Rockefeller, the JPB Foundation, Leon Levy Foundation, Open Society Foundations, Rockefeller Brothers Fund, and Wallace Global Fund for their generous support of our election security work.

The authors would like to thank the many colleagues who collaborated in preparing this tool kit. Derek Tisler, Christopher Deluzio, and Wilfred Codrington contributed crucial research and editorial support to this project. Research and Program Associates Brianna Cea, Shyamala Ramakrishna, and Andrea Córdova McCadney merit special thanks for their sustained assistance in researching, fact-checking, and editing.

We are also indebted to the many experts and officials whose knowledge and feedback helped shape this tool kit. We gratefully acknowledge the following individuals for sharing their insights: Pam Smith, senior adviser, Verified Voting; Whitney Quesenbery, codirector, Center for Civic Design; Dana Chisnell, codirector, Center for Civic Design; Marcia Johnson-Blanco, codirector, Lawyers' Committee for Civil Rights Under Law; Laura Grace, election protection manager, Lawyers' Committee for Civil Rights Under Law; Michelle Bishop, disability advocacy specialist for voting rights, National Disability Rights Network; Aquene Freechild, campaign codirector, Public Citizen; Emily Berger, senior fellow, Public Citizen; Susannah Goodman, director of election security, Common Cause; Neal Kelley, registrar of voters, Orange County, California; Noah Praetz, director of elections, Cook County, Illinois; Matthew Davis, former chief information officer, Virginia Department of Elections; Dana DeBeauvoir, county clerk, Travis County, Texas; Genya Coulter, precinct clerk at Polk County [Florida] Supervisor of Elections; Tonia A. Tunnell, director of government relations, Maricopa County [Arizona] Recorder's Office and Elections Department; Maribeth Witzel-Behl, city clerk, Madison, Wisconsin; Richard Rydecki, assistant administrator, Wisconsin Elections Commission; Susan Greenhalgh, national policy director, National Election Defense Coalition; and Maurice Turner, senior technologist, Center for Democracy & Technology.

BRENNAN
CENTER
FOR JUSTICE

Brennan Center for Justice at New York University School of Law
120 Broadway // 17th Floor // New York, NY 10271
www.brennancenter.org

The CHAIRPERSON. Thank you very much.

Dr. Blaze, we'd love to hear from you.

TESTIMONY OF MATT BLAZE

Mr. BLAZE. Thank you, Chairperson Lofgren and Ranking Member Davis, for convening this hearing on the urgently important topic of securing America's elections.

I come here today as a computer scientist who's spent the better part of the last quarter-century studying election system security.

As you are well aware, the integrity of elections across the U.S. depends heavily on the integrity of computers and software systems that are embedded across our election infrastructure. Complex software lies at the heart not just of vote-casting equipment used at polling places but also the information systems used by local authorities to manage everything from voter registration records to the tallying and reporting of election results, to the creation of ballots and so forth.

Unfortunately, much of this infrastructure has proven dangerously vulnerable to tampering and attack and, in some cases, in ways that cannot be easily detected or corrected after the fact. These vulnerabilities can create practical avenues for corrupt candidates or foreign adversaries to do everything from cause large-scale disruption on election day to potentially undetectably alter election outcomes in some cases.

Now, for the purpose of my testimony, it's helpful to consider voting machines and election management infrastructure separately. Let me begin with the voting equipment itself.

To be blunt, it's a widely recognized indisputable fact that every piece of computerized voting equipment in use at polling places today can be easily compromised in ways that have the potential to disrupt election operations, compromise firmware and software, and potentially alter vote tallies in the absence of other safeguards.

This is partly a consequence of historically poor design and implementation by equipment vendors, but it's ultimately a reflection of the nature of complex software. It's simply beyond the state of the art to build software systems that can reliably withstand targeted attack by a determined adversary in this kind of an environment.

The vulnerabilities are real, they're serious, and, absent a surprising and very fundamental breakthrough in my field, which I would welcome but I don't see coming soon, probably inevitable.

Fortunately,—this is not all bad news—there is now overwhelming consensus among experts on how we can conduct reliable elections despite the inherent unreliability of the underlying software. This requires two things.

The first is that the voting technology retain a reliable paper record that reflects the voters' intended choices. Fortunately, equipment that has this property exists today, and it's, in fact, the simplest of the voting equipment available. And I refer here to paper ballots that have been preferably marked by hand, when possible, that are fed into an optical scan ballot reader when the vote is cast and the original voter ballot is retained.

But this isn't sufficient by itself, because the software in the ballot scanners is, itself, vulnerable to tampering or error.

The second requirement is that the election be reliably audited to ensure that the software is reporting the correct outcomes of each race as defined by the ballots that the voter has marked. And there's a statistically rigorous technique called risk-limiting audits that you've heard about that can accomplish this effectively and quickly. But this has to be routinely performed after every election in order to provide meaningful assurance.

Unfortunately, only a handful of States currently conduct these audits. And it's urgent that both of these safeguards—paper ballots and risk-limiting audits—recognized by experts universally as essential for election integrity, be adopted quickly and widely throughout the Nation.

The second technology is the election management infrastructure in use by jurisdictions. We give most of the attention to vulnerabilities in voting machines, but that's not the whole story. Each of the more than 5,000 jurisdictions responsible for running elections across the Nation must maintain a number of critical information systems that are attractive targets for disruption by adversaries. Most important of these are voter registration databases, the systems that report final results and so forth.

Unfortunately, there are even fewer standards for how to secure these systems. The administration of these systems varies widely. And the threats against these systems are often even more acute than the threats against individual voting systems.

You know, just as we don't expect the local sheriff to single-handedly defend against military ground invasions, we shouldn't expect county election IT managers to defend against cyber-attacks by foreign intelligence services, but that's precisely what we've been asking them to do.

Thank you again for your attention to these important issues. This is a vitally important topic, and I'm grateful that you've invited me to testify.

[The statement of Mr. Blaze follows:]

MATT BLAZE [1]

TESTIMONY BEFORE THE
US HOUSE OF REPRESENTATIVES
COMMITTEE ON HOUSE ADMINISTRATION

HEARING ON
"2020 ELECTION SECURITY – PERSPECTIVES FROM VOTING SYSTEM VENDORS AND EXPERTS"

JANUARY 9, 2020

[1] McDevitt Professor of Computer Science and Law, Georgetown University, 600 New Jersey Ave NW. Washington, DC 20001. *mab497@georgetown.edu.* Affiliation for identification only.

INTRODUCTION

Thank you for the opportunity to offer testimony on the important questions raised by the security of the technology used for elections in the United States.

For more than 25 years, my research and scholarship has focused on security and privacy in computing and communications systems, especially as we rely on insecure platforms such as the Internet for increasingly critical applications. My work has focused particularly on the intersection of this technology with public policy issues. For example, in 2007, I led several of the teams that evaluated the security of computerized election systems from several vendors on behalf of the states of California and Ohio.

I am currently the McDevitt Professor of Computer Science and Law at Georgetown University. From 2004 to 2018, I was a professor of Computer and Information Science at the University of Pennsylvania. From 1992 to 2004, I was a research scientist at AT&T Bell Laboratories. I hold a PhD in computer science from Princeton University, an MS in computer science from Columbia University, and a BS from the City University of New York. This testimony is not offered on behalf of any organization or agency.

In this testimony, I will give an overview of the technical security risks facing elections in the United States today, with emphasis on vulnerabilities inherent in electronic voting machines, as well as the exposure of our election infrastructure to disruption by domestic as well as national security adversaries[2]. I have attempted, to the extent possible, to represent the current consensus of experts in the field, but space and time constraints limit my ability to be comprehensive or complete. An especially valuable resource, with comprehensive discussion and recommendations. is the recent National Academies "Securing the Vote" consensus study report.[3]

I offer three central recommendations:

- Paperless ("DRE") voting machines should be phased out from US elections immediately, and urgently replaced with precinct-counted optical scan ballots that leave a direct artifact of voters' choices.
- Statistically rigorous "risk limiting audits" should be routinely conducted after *every* election, in *every* jurisdiction, to detect and correct software failures and attacks.
- State and local voting officials should be provided significant additional resources, infrastructure, and training to help them protect their election management IT systems against increasingly sophisticated adversaries.

[2] My testimony is focused on technical vulnerabilities and threats specific to the voting process itself, and does not attempt to cover other serious threats to elections, even though they may leverage modern technology (such as, for example, disinformation campaigns that exploit digital media).

[3] https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

I. Elections and Software Security

A consequence of our federalist system is that US elections are in practice highly decentralized, with each state responsible for setting its own standards and procedures for registering voters, casting ballots, and counting votes. The federal government has set only broad standards for such issues as accessibility, but has historically been largely uninvolved in day-to-day election operations. In most states, the majority of election management functions are delegated to local county and town governments, which are responsible for registering voters, procuring voting equipment, creating ballots, setting up and managing local polling places, counting votes, and reporting the results of each contest. Consequently, thousands of individual local election offices shoulder the burden of managing and securing the voting process for most of the American electorate.

Elections in the US are among the most operationally and logistically complex in the world. Many jurisdictions have large numbers of geographically dispersed voters, and most elections involve multiple ballot contests and referenda. Baseline election security must account for sophisticated adversaries, ballot secrecy, fair access to the polls, and accurate reporting of results, making secure election management one of the most formidable – and potentially fragile – information technology problems in government

Computers and software play central roles in almost every aspect of our election process: managing voter registration records, defining ballots, provisioning voting machines, tallying and reporting results, and controlling electronic voting machines used at polling places.[4] The integrity and security of our elections are thus inexorably tied to the integrity and security of the computers and software that we rely on for these many functions.

The passage of the Help America Vote Act (HAVA) in 2002 accelerated the computerization of voting systems, particularly with respect to the ways in which voters cast their ballots at local polling stations. HAVA provided funds for states to replace precinct voting equipment with "accessible" technology. As implemented, however, some of this new technology has had the unfortunate unintended consequence of increasing, rather than decreasing, the risk of our elections being compromised by malicious actors.

A. Election Software and Hardware

A typical[5] county election office today depends on computerized systems and software for virtually every aspect of registering voters and conducting elections. Generally, an election office workflow will include at least the following pre- and post- election functions:

Voter registration – The ongoing maintenance of an authoritative database of registered voters in the jurisdiction, including the precinct-by-precinct "poll books" of voters (which

[4] A typical election administration office is much like any modern enterprise, with local computer networks tying together desktop computers, printers, servers, and Internet access. This increasing connectivity served as a critical avenue in 2016 for what US intelligence agencies have identified as attacks by Russian military intelligence..

[5] The precise nature of the systems used and how they interact with one another will vary somewhat depending on the vendors from which the systems were purchased and the practices of the local jurisdiction.

might be on paper or in electronic form) that are used to check in voters at precinct polling stations.

Ballot definition – The pre-election process of creating data files that list the various contests, candidates, and rules (e.g., number of permitted choices per race) that will appear on the ballot. The ballot definition is used to print paper ballots, to define what is displayed on touchscreen voting terminals, and to control the vote tallying and reporting software. Local races (such as school boards) may sometimes require that different ballot definitions be created for different precincts within a county in any given election.

Voting machine provisioning – The pre-election process of configuring the individual precinct voting machines for an election. This typically includes resetting internal memory and loading the appropriate ballot definition for each precinct. Depending on the model of voting machine, provisioning typically involves using a computer to write removable memory cards that are installed in each machine.

Absentee and early voting ballot processing – The process of reading and tabulating ballots received by mail and from early voting polling places. Mail votes are typically processed in bulk by high-volume optical scan ballot reading equipment.

Tallying and reporting – The post-election process of tabulating the results for each race received from each precinct and reporting the overall election outcomes. This process typically involves using a computer to read memory card media retrieved from precinct voting machines.

Each of the above "back end" functions employs specialized election management software running on computers. Depending on the size and practices of the county, the same computers may be used for more than one function (e.g., the ballot definition computer might also serve as the tallying and reporting computer). These computers are typically off-the-shelf desktop machines running a standard operating system (such as Microsoft Windows), often equipped with electronic mail and web browser software along with the specialized voting software. Election office computers are typically connected to one another via a wired or wireless local area network, which may have a direct or indirect connection (sometimes via a firewall) to the Internet.

In some jurisdictions, some or all of these election management functions (most typically those concerned with voter registration databases and ballot definition), may be outsourced by a county or state to an election services contractor. These contractors provide jurisdictions with specialized assistance with such tasks as creating ballots in the correct format, managing voter registration databases, creating precinct poll books, and maintaining voting machines. The degree to which jurisdictions rely on outside contractors varies widely across the nation.

Much of the voting equipment used at precincts is computerized as well, although it is generally packaged in specialized hardware. This equipment includes:

Direct Recording Electronic (DRE) Voting Machines – DRE machines are special-purpose computers that display ballot choices to the voter (based on the ballot definition) and record voter choices. Both the ballot definition configuration and the vote count are typically stored on removable memory media.[6]

[6] Some models of DRE can be equipped with a *Voter Verified Paper Audit Trail (VVPAT)* option in which the

Optical Scan Ballot Readers – Optical scan ballot readers are specialized computers that read voter-marked paper ballots. The ballot is read according to the ballot definition configuration (typically on removable memory media), and a tally is maintained in memory (also typically on removable media). The machine also captures the scanned ballots and stores them in a mechanically secured ballot box.

Ballot Marking Devices (BMDs) – Ballot marking devices are an assistive technology used in optical scan systems to allow visually or mobility impaired voters to create ballots for subsequent scanning. BMDs are similar in appearance to DRE machines in that they display (or read aloud) the ballot electronically, based on a ballot definition configuration, and accept voter choices for each race. However, instead of recording those choices in computer memory as DREs do, BMDs print a marked paper ballot that can then be submitted through an optical scan ballot reader.

Electronic Poll Books – These devices are typically tablet-style computers that contain an authoritative copy of the database of registered voters at each precinct. Electronic poll books are not used directly by voters, but rather by precinct poll workers as voters are checked in at their polling place. They are not used in all jurisdictions.

B. *Software and Election Security*

Securing complex software systems is notoriously difficult, and those that perform the various functions described above are no exception.[7] There are several avenues of vulnerability in such systems. Common software "bugs" often introduce vulnerabilities that can be exploited by an adversary to silently compromise the integrity of data or make unauthorized (and difficult to detect) changes to the behavior of systems. Configuration and system management errors (such as the use of vulnerable out-of-date platforms and weak passwords) can further compromise security. Computer networks (which are not generally used by precinct voting machines themselves but are commonly connected to back end systems in election offices) compound these risks by introducing the possibility of remote attack over the Internet.

The integrity of the vote today thus increasingly depends on the integrity of the software systems – running on voting machines and on county election office networks – over which elections are conducted. Any security weakness in any component of any of these systems can serve as a "weak link" that can allow a malicious actor to disrupt election operations, alter tally results, or disenfranchise voters.

In many electronic voting systems used today, a successful attack that exploits a software flaw might leave behind little or no forensic evidence. This can make it effectively impossible to determine the true outcome of an election or even that a compromise has occurred.

voters' selections are printed on a paper tape roll that is visible to the voter. VVPATs can assist with determining the voter's intent during a recount, but their efficacy depends on each voter's diligence in confirming that their choices are correctly recorded on the paper tape before they leave the voting booth. Research consistently suggests that, in practice, very few voters successfully perform this confirmation step.

[7] The fact that software systems can be, and often are, vulnerable to attack is not unique to election systems, of course. Serious data breaches are literally daily events across the public and private sectors, and cybersecurity is widely recognized to be a serious law enforcement and national security problem. To the extent that elections depend on software or are administered by networked computing systems, they are subject to all the same risks.

Unfortunately, these risks are not merely hypothetical or speculative. Many of the software and hardware technologies that support US elections today have been shown to suffer from serious and easily exploitable security vulnerabilities that could be used by an adversary to alter vote tallies or cast doubt on the integrity of election results.

II. Current Electronic Voting Systems Have Proven Vulnerable to a Range of Known, Exploitable Security Flaws

A. Risks in Various Election Components

Security concerns about computerized voting systems have been raised from almost the moment such systems were first proposed. Most of these concerns have focused on electronic voting equipment used at polling stations, although the "back end" election management software used to manage voter registration, provision voting machines, and tally are at least equally critical to the integrity of the vote.

To be clear, all current electronic voting technology can and does suffer from security vulnerabilities. The consequences of these vulnerabilities being successfully exploited, however, depend on the particular class of device and whether the technology permits effective post-election auditing to validate or recover correct election results and detect anomalies.

1. Election Management IT Systems

As noted in the previous section, local jurisdictions rely on computers for almost every aspect of election administration. Official information for voters is distributed on public-facing websites. Voter registration records, used on election day to determine who is permitted to vote, are maintained in computerized databases. Ballots forms are created and edited on computers. Absentee ballot mailings are managed by computer. Preliminary and official election results are maintained and disseminated by computer. Specialized "Election Management" software (generally provided by the vendor of the jurisdiction's voting equipment) is used to configure ballots and read results from precinct voting machines.

In most cases, the computers used for election administration employ the same hardware, operating systems, and networking platforms employed by other enterprises, and may be connected, directly or indirectly[8], to the Internet. Election management systems are exposed to the same risks of compromise by malicious actors that cause the commonplace "data breaches" seen in other private and public sector domains that have become regular fixtures of online life.

Many jurisdictions outsource some of their election management tasks to outside vendors or contractors. This practice amplifies the exposure of election infrastructure to external tampering.

Disruption or compromise of any local election administration functions can have grave (and often non-recoverable) consequences for the integrity of elections. Compromise of voter registration databases can be exploited by adversaries to cause long lines at polling places (forcing large numbers of voters to cast provisional ballots) and can selectively disenfranchise voters to favor particular candidates. Provisioning of voting machines with incorrect ballot definitions can prevent correct ballots from being cast. Errors in in unofficial or final tallies can cast doubt on the legitimacy of entire elections. In some cases, successful attacks may not be discovered until long after polls have closed, or may never be discovered at all.

[8] Most election jurisdictions, like other enterprises, employ "firewalls" between their internal networks and the public Internet. However, firewalls are not by themselves in a complete or sufficient defense against remote attack.

The IT and security administration of election management computers varies widely from jurisdiction to jurisdiction. In the best cases, there may be a full-time staff devoted to securing and managing election computers and networks. In a more typical case, computer security is relegated to the general county IT staff, which may have only limited resources relative to the threat. In all cases, however, even the best defensive cybersecurity resources of a local county are of only limited value against a foreign state adversary.

Local election management computers and networks are especially attractive targets for foreign tampering and interference. They can often be attacked remotely, without the need for physical presence in the targeted jurisdiction, and successful attacks may be rewarded with partial or complete control over a county's voter registration databases, voting machine configuration, and results reporting infrastructure.

2. Electronic Poll Books

Electronic poll books, which are not used in every jurisdiction, perform the initial voter "check in" function at polling places on election day. They must, by nature of their function, have reliable access to an authoritative list of the voters registered to vote at each polling place. This may be accomplished either with an internal copy of the voter registration database or by online remote access to a central computer. In either configuration, electronic poll books perform an essential election function and must be reliably secured against tampering. If poll books are unavailable or if their databases are corrupted, voters will not be able to cast ballots (except by provisional ballot, to the extent that is a viable option).

Electronic poll books have received much less scrutiny than other precinct voting equipment, but are subject to all the same risks and attack vectors as other electronic devices. In many jurisdictions, they are largely unregulated and require little or no outside certification or audit.

3. Optical Scan Ballot Readers

Optical scan ballot readers are specialized computers that scan and retain printed ballots and record on electronic storage media the tally of votes cast in each race. They depend on the integrity of their software and hardware for their ability to correctly interpret ballots and to correctly record votes. They are exposed to physical access by poll workers, and, in many cases, individual voters.

Ballot scanners can be compromised in a number of practical ways, any one of which can compromise the recorded vote tally. However, because they retain the physical paper ballots marked by voters, it is possible to recover from such a compromise if it is detected. A technique called "risk-limiting audits" can reliably detect and recover from defective or compromised ballot scanners and is discussed in the sections that follow.

4. Ballot Marking Devices

Originally, Ballot Marking Devices (BMDs) were conceived of narrowly, as an assistive technology for use by voters with disabilities to assist them in marking optical scan paper ballots, (bringing such systems into compliance with Help America Vote Act (HAVA) requirements for accessible voting). However, certain recent voting products greatly expand the use of BMD technology by integrating a BMD into the voting process for all voters, whether they require assistive technology or not.

BMD-based voting systems are controversial, since, by virtue of their design, the correctness of their behavior cannot be effectively audited except by individual voters carefully verifying their machine-printed ballots before they are cast. A maliciously compromised BMD could subtly mismark candidate selections on ballots in a way that might not be noticed by most voters and that could undetectably change election outcomes. Furthermore, if BMDs fail or must be rebooted at a polling place, there may be no alternative method for voters to create marked ballots, making BMDs a potential bottleneck or single point of failure on election day.

As a relatively new technology, BMD-based systems have not yet been widely examined by independent researchers and have been largely absent from practical election security research studies. However, even with relatively little scrutiny, exploitable weaknesses and usability flaws have been found in these systems, This underscores the need for more comprehensive studies and for caution before these systems are purchased by local jurisdictions or widely deployed.

5. Direct Recording Electronic (DRE) Voting Machines

From a security perspective, by far the most problematic and risky class of electronic voting systems are those that employ *Direct Recording-Electronic (DRE)* machines. DRE machines are special purpose computers programmed to present the ballot to the voter and record the voter's choices on an internal digital medium such as a memory card. At the end of the election day, the memory card containing the vote tallies for each race is generally removed or electronically read from the machine and delivered to the county election office, where the tallies from each precinct are recorded by the county tallying software. DRE machines are sometimes informally called "touchscreen" voting machines, although not all DRE models use actual touchscreen displays (nor are all election devices that employ touchscreens DREs).

The design of DREs makes them inherently difficult to secure and yet also makes it especially imperative that they *be* secure. This is because the accuracy and integrity of the recorded vote tally depends completely on the correctness and security of the machine's hardware, software, and data. Every aspect of a DRE's behavior, from the ballot displayed to the voter to the recording and reporting of votes, is under control of the DRE hardware and software. Any security vulnerability in this hardware or software, or any ability for an attacker to alter (or re-load new and maliciously behaving) software running on the machine, not only has the potential to alter the vote tally, but can make it impossible to conduct a meaningful recount (or even to detect that an attack has occurred) after the fact. If a DRE is compromised at any time before or during an election, any votes cast on it are irreparably compromised as well.

DRE-based systems introduce several avenues for attack that are generally not present (or are not as security-critical) in other voting technologies:

- Alteration or deletion of vote tallies stored in internal memory or removable media
- Alteration or deletion of ballot definition parameters displayed to voters [9]
- Alteration or deletion of electronic log files used for post-election audits and detecting unauthorized tampering

Attacks might be carried out in any of several ways, each of which must be reliably defended against by the DRE hardware and software:

- Direct tampering with data files stored on memory cards or accessible through external interface ports
- Surreptitious replacement of the certified software running on the device with a maliciously altered version
- Exploitation of a pre-existing vulnerability in the certified software

Successfully exploiting just *one* of these avenues of attack can be sufficient to undetectably compromise an election. The design of DREs makes it necessary not only that their hardware be highly secure against unauthorized tampering, but that the software running on them not suffer from *any* vulnerabilities that could be exploited by a malicious actor. This makes the security requirements for DREs more stringent – and also more easily defeated – than for any other currently deployed election technology.

Unfortunately, the DRE-based systems purchased by (and still used in) various states under HAVA have repeatedly been found to suffer from exactly these kinds of exploitable hardware and software vulnerabilities.

B. The 2007 California and Ohio Studies

To date, the most extensive independent studies of the security of electronic voting systems were commissioned in 2007 by the Secretaries of State of California and Ohio. Expert review teams were given access to the voting machine hardware and software source code of every system certified for use in those states. The systems used in California and Ohio were also certified for use in most of the rest of the country, so these studies effectively covered a large fraction of available electronic voting equipment and software. I led the teams that reviewed Sequoia products (for the state of California) and ES&S products (for the state of Ohio); other teams in these studies reviewed Diebold/Premier and Hart InterCivic products.[10]

[9] An incorrect (or maliciously altered) DRE ballot definition can make it impossible to determine the true election results even without any malicious software exploitation. For example, in York County, PA, a DRE ballot definition programming error in the 2017 general election appears to have allowed candidates in some local races to be voted for twice, with the possible consequence that the election will have to be invalidated and redone. See http://www.ydr.com/story/news/2017/11/08/voting-machine-problems-what-york-countys-options/843423001/ . Paper-based systems, in contrast, are more robust against such errors. For example, the 2000 general election in Bernalillo County, NM had a similar error in their punch card counting software, but was later able to correct the error without a new election; see https://www.wsj.com/articles/SB976838091124686673

[10] The various final reports of the California "Top-To-Bottom Review" studies can be found at http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/ . The final report of the Ohio "Project EVEREST" study can be found at https://www.eac.gov/assets/1/28/EVEREST.pdf

In both studies, every team found and reported serious, exploitable vulnerabilities in *almost every component* examined. In most cases, these vulnerabilities could be exploited by a single individual, who would need no more access than an ordinary poll worker or voter to carry out effective attacks. Such an attacker would be able to alter vote tallies, load malicious software, or erase audit logs. Some of the vulnerabilities found were the consequence of software bugs, while others were caused by fundamental architectural properties of the system architecture and design. In some cases, compromise of a single system component (such as a precinct voting machine) was sufficient to compromise not just the vote tally on that machine, but to compromise the entire county back end system.

In response, California and Ohio ordered some equipment decertified and some election-day procedures modified. However, all the vulnerable equipment and software remained certified for use in at least some other states.

Some equipment vendors and local voting officials claimed at the time that the findings of the California and Ohio studies were irrelevant or overstated, that any problems identified could be easily fixed, and that it would be difficult or impossible for anyone but an expert with extensive experience and access to privileged information (such as source code) to exploit vulnerabilities in practice. However, as exercises such as the DEFCON Voting Village (described below) have demonstrated, not only do these systems remain vulnerable, but they can be readily exploited by people with no more than ordinary, undergraduate-level computer science experience and expertise, and without access to any secret or proprietary information.

C. The DEFCON Voting Village Exercise

The DEFCON conference is one of the world's largest and best-known computer security "hacker" conferences. Last year's DEFCON was held August 8-10, 2019, in Las Vegas, NV, and drew more than 25,000 participants from around the world. DEFCON participants have broad interest in technology, and include security researchers from industry, government, and academia, as well as individual hobbyists.

For the last three years, DEFCON has featured a *Voting Machine Hacking Village* ("Voting Village") to give participants an opportunity to examine and get hands-on experience with the security technology used in US elections, including voting machines, voter registration databases, and election office networks. I am one of the organizers of the Voting Village.[11]

The voting machines available in the Voting Village included a variety of DRE, optical scan readers, ballot marking devices and electronic poll books from a range of commercial vendors. We acquired (from the surplus market) and made available to participants a sampling of different pieces of election hardware, including both DRE and optical scan voting machines as well as "poll book" devices used by used by precinct workers to verify and check in voters at polling places. Every model machine currently at the Voting Village is still certified for use in U.S. elections in at least one jurisdiction today.

[11] Organizers of the DEFCON Voting Village include the author as well as Harri Hursti, Margaret MacAlpine, and Jeff Moss.

The DEFCON Voting Village is not intended to be a formal security assessment or test, but rather an opportunity for a general audience of technologists to examine election equipment and systems. However, participants are encouraged to critically examine and probe the equipment and software for vulnerabilities, and to seek practical ways to compromise security mechanisms. No proprietary information or computer source code is made available.

The results of the Voting Village are summarized each year in detail in a report.[12] It is notable that participants, who overwhelmingly do not have any previous special expertise in voting machines or access to any proprietary information about them, have been very quickly able to find ways to compromise *every* piece of equipment in the Village by the end of the weekend. Depending on the individual model of machine, participants have found ways to load malicious software, gain access to administrator passwords, compromise recorded votes and audit logs, or cause equipment to fail. In most cases, these attacks could be carried out from the ordinary interfaces that are exposed to voters and precinct poll workers.

The ease with which participants compromise equipment in the Voting Village should be regarded as at once alarming and yet also unsurprising. It is alarming because the very same equipment is in use in polling places around the United States, relied on for the integrity of real elections. But it is also ultimately unsurprising. Versions of many of the machines at DEFCON had been examined in the 2007 studies and found to suffer from basic, exploitable security vulnerabilities. It should not come as any surprise that, given access and motivation, people of ordinary skill in computer security would be able to replicate and expand on these results. It is, in fact, precisely what the previous studies of these devices warned would happen.

In summary, the DEFCON Voting Village demonstrates that much of the voting technology used in the US is vulnerable not just to hypothetical expert attack in a laboratory environment, but also to practical analysis, manipulation and exploitation by non-specialists with only very modest resources.

[12] The current Voting Village final report is available at: https://media.defcon.org/DEF%20CON%2027/voting-village-report-defcon27.pdf

III. US Election Systems Are Not Engineered to Resist National Adversaries

The traditional "threat model" against which electronic voting systems have been evaluated has been largely focused on resisting traditional election *fraud*, in which domestic conspirators, perhaps assisted by corrupt poll workers or election officials, attempt to "rig" an election to favor a preferred candidate in a local, state, or national contest. Fraud might be accomplished by altering votes, adding favorable votes, deleting unfavorable votes, or otherwise compromising the security mechanisms that protect the ballot and tally.

While virtually every study of electronic voting technology has raised questions about the ability of current systems to resist serious efforts at fraud, traditional election fraud is not the only kind of threat, or even the most serious threat, that a voting systems must resist today.

Electronic voting systems must resist not only fraud from corrupt candidates and supporters, but also election *disruption* from hostile foreign adversaries. This is a much more formidable threat, and one that current systems are far less equipped to resist.

The most obvious difference between traditional election fraud by corrupt domestic actors and disruption by hostile state actors is the expected resources and capabilities available to each. The intelligence services of even small nations can marshal far greater financial, technical, and operational resources than would be available to even highly sophisticated criminal conspiracies. For example, intelligence services can feasibly conduct advance operations against the voting system *supply chain*. In such operations, the aim might be to obtain confidential source code or to secure surreptitious access to equipment before it is even shipped to local election officials. Hostile intelligence services can exploit information and other assets developed broadly over extended periods of time, often starting well before any specific operation or attack has been planned.

But their greater resources are not the most important way that hostile state actors can be a more formidable threat than corrupt candidates or poll workers. They also enjoy easier goals. The aim of traditional "retail" election fraud is to tilt the outcome in favor of a particular candidate. That is, to succeed, the attacker must generally alter the reported vote count or add, change, or delete votes. But a hostile state actor – via an intelligence service such as Russia's GRU – might be satisfied with merely *disrupting* an election or calling into question the *legitimacy* of the official outcome. With election systems so heavily dependent on demonstrably insecure software and voting equipment, this kind of disruption could be comparatively simple to accomplish, even at a national scale.

A hostile state actor who can compromise even a handful of county networks might not need to alter any actual votes to create widespread uncertainty about an election outcome's legitimacy. It may be sufficient to simply plant suspicious (and detectable) malicious software on a few voting machines or election management computers, create some suspicious audit logs, delete registered voters from the rolls, or add some obviously spurious names to the voter rolls. If the preferred candidate wins, they can simply do nothing (or, ideally, use their previously arranged access to restore the compromised networks to their original states, erasing any evidence of compromise). If the "wrong" candidate wins, however, they could covertly reveal evidence that county election systems had been compromised, creating public doubt about whether the election had been "rigged". This could easily impair the ability of the true winner to effectively govern, at least for a period of time.

Electronic voting machines and vote tallies are not the only potential targets for such attacks. Of particular concern are also the "back end" systems that process voter registration, ballot definition, and other election management tasks. Compromising any of these systems (which are often connected, directly or indirectly, to the Internet and therefore potentially remotely accessible) can be sufficient to disrupt an election while the polls are open or cast doubt on the legitimacy of the reported result. The decentralization of election operations, managed by thousands of individual local offices throughout the nation (with widely varying resources) is sometimes cited as a strength of our electoral process. However, this decentralization can be turned to the adversary's advantage. An attacker can choose arbitrarily from among whatever counties have the weakest systems – those with the least secure software or most poorly defended networks and procedures – to target.

It is beyond the scope of my testimony to speculate on specific intrusions that occurred against state and local election management systems in the 2016 US general election, much of which remains classified or under investigation. It has been reported that voter registration management systems in at least several states were targeted for exploitation and access. It is unclear whether voting machines or tallying systems were also targeted. However, targeting and exploiting such systems would have been well within the capability of any major rival intelligence service.[13]

In summary, the architecture of many current electronic voting systems, especially those that employ DRE voting machines, makes disruption attacks an attractive option for our foreign adversaries – and an especially difficult one to effectively defend against. These systems can give hostile actors interested in disruption an even *easier* task than that facing corrupt candidates seeking to steal even a small local office. And the consequences of election disruption strike at the very heart of our national democracy.

[13] For a comprehensive discussion of technical attacks against our election infrastructure in 2016, see the Report of the Select Committee on Intelligence, US Senate on Russian Active Measures in the 2016 US Election, Vol 1. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf

IV. Recommendations: All US Elections Should Employ Paper Ballots and Risk-Limiting Audits

It is perhaps tempting to conclude pessimistically that election technology in the US is fatally flawed, leaving our nation irreparably vulnerable to election fraud and foreign meddling. But while it is true that the current situation exposes us to significant risk, it is by no means hopeless or beyond repair. Relatively simple, and available, technologies can be deployed that render our elections significantly more robust in the face of attack.

While electronic voting machines do indeed suffer demonstrably fundamental weaknesses, some electronic voting technologies are significantly more resilient in the face of compromise than others. The most important feature required is that there be a reliable record of each voter's true ballot selections that can be used as the basis for a post-election audit to detect and recover from failure or compromise of the software or hardware.

Among currently available, HAVA-compliant voting products, the only systems that meet this requirement are those that employ *optical scan paper ballot* technology. In such systems, the voter fills out a machine-readable paper ballot form (possibly with the aid of an assistive ballot marking device for language-, visually- and mobility-impaired voters), that is then deposited into a ballot scanning device that reads the ballot choices, maintains an electronic tally, and retains and secures the marked paper ballots for subsequent audit. After the polls close, the electronic tally records are read from each ballot scanner and preliminary results calculated.

The paper records of votes that precinct-counted optical-scan systems provide are a necessary, but not by themselves sufficient, safeguard against software. As noted above, even non-DRE systems can suffer from flaws and exploitable vulnerabilities in the voting machine and back end software. The second essential safeguard is a systematic and reliable process for detecting whether the software has reported incorrect results, and to recover the true results if so.

The most reliable and well-understood method to achieve this is through an approach called *risk-limiting audits*.[14] In a risk limiting audit, a statistically rigorous method is used to select a randomized sample of ballots, which are manually checked by hand and compared with their electronic interpretation. (This must be done for *every* contest, not just those with close results that might otherwise call for a traditional "recount".) If discrepancies are discovered between the manual and electronic tallies, additional manual checks are conducted. The effect of risk-limiting audits is not to eliminate software vulnerabilities, but to ensure that the integrity of the election outcome does not depend on the herculean task of securing every software component in the system. This important property is called *strong software independence*.[15]

It is worth emphasizing that risk-limiting audits are only meaningful if there is a reliable, human-readable artifact of the voters' true selections, such as is provided by paper ballots that have been directly marked by the voter.

[14] A comprehensive overview of risk-limiting audits is beyond the scope of this testimony. A good introduction to their theory and practice can be found at https://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf .

[15] See Ron Rivest. "On the notion of 'software independence' in voting systems". *Phil. Trans Royal Society A*. Volume 366 Issue 1881. October 28, 2008. http://rsta.royalsocietypublishing.org/content/366/1881/3759 .

Optical scan paper ballots and risk-limiting audits comprise a critical, and readily deployable, safeguard against both traditional election fraud and national security threats. Taken together, they permit us to more safely enjoy the benefits of computerized election management, without introducing significant new costs or requiring the development of speculative new technology. The technology required for this is available *today*, from multiple vendors, and is already in use in many states. In jurisdictions that already use optical scan ballots, implementing effective risk-limiting audits is entirely a procedural matter. In those that do not, it will also require the investment in new precinct voting equipment.

As important as paper ballots and risk-limiting audits are, however, they are not panaceas that solve every threat to our elections. It is equally critical that the state and county computer infrastructure used for election management and voter registration be vigilantly protected against compromise. As we saw in 2016, hostile actors – whether foreign or domestic – might attempt to breach not just voting machines, but also back end election management systems and voter registration database systems, which are often exposed to remote attack over the Internet.

It is no exaggeration to observe that state and local election officials serve on the front lines of our national cybersecurity defense. They must be given sufficient resources, infrastructure, information, and training to help them effectively defend their systems against an increasingly sophisticated – and increasingly aggressive – threat environment. It is notable that the budgets for election administration often must compete for resources with essential local services such as fire protection and road maintenance. Election management represents only a miniscule fraction of the total national spending on political campaigns. Additional investment here will pay significant dividends for our security.

By analogy, we do not make the county sheriff responsible for defending against ground invasions by foreign military forces. Yet that is precisely the role into which we have placed our local county IT administrations in defending our election infrastructure against electronic attacks. Without significant national-level support, we are setting them up for failure.

Simply put, much of our election infrastructure remains vulnerable to practical attack, with threats that range from traditional election tampering in local races to large-scale disruption by national adversaries. We should take no comfort if such attacks have not yet been widely detected. At best, it is only because, for whatever reason, serious attempts have not yet been made. Given the potential rewards to our adversaries, it is only a matter of time before they will.

National-level investment in safeguards such as those described above serve our democracy in critically important ways. They can provide a significant improvement to election security, both in our ability to resist attack and in our ability to recover from attacks when they occur. Perhaps most importantly, they provide meaningful assurance to voters that their ballots truly count and that their elected officials are governing truly legitimately. Our republic cannot long survive without the confidence that comes from that assurance.

The CHAIRPERSON. Thank you very much, Dr. Blaze.

Dr. Gilbert.

TESTIMONY OF JUAN GILBERT

Mr. GILBERT. Chairperson Lofgren, Ranking Member Davis, Members of the Committee, I am honored to share with you my expertise in voting system security, accessibility, and usability.

I have worked in elections for more than 15 years, conducting research, developing innovative technologies, and conducting studies with various election stakeholders.

In 2003, I created Prime III, an open-source universally designed system. To my knowledge, Prime III is the only open-source voting system to be used in State, Federal, and local elections in the United States. New Hampshire adopted Prime III, renamed it as "One4All," and Butler County, Ohio, uses it as their accessible absentee system. Furthermore, voting machine vendors have created ballot-marking systems modeled after Prime III.

While I am appearing today in my capacity as an expert in voting systems, I would like to take this opportunity to share some key recommendations from the 2018 National Academies of Science, Engineering, and Medicine consensus report titled "Securing the Vote: Protecting American Democracy."

I was a member of the committee that authored the report, but I would emphasize that any opinions expressed about the report and its recommendations are my own and do not necessarily represent positions of the National Academies.

"Securing the Vote" was the result of a two-year National Academies study conducted by experts from election administration and policy, cybersecurity, accessibility, and law. Over the course of the study, the committee reviewed extensive background materials. It held five meetings where invited experts spoke to the committee about a range of topics, including voter registration, accessibility, voting technologies, market impediments to technological innovation, cybersecurity, post-election audits, and the education and training of election workers.

The committee did not have access to classified information but instead relied on information in the public domain, including State and Federal Government reports, published academic literature, testimony from congressional hearings, and presentations to the committee.

Issues related to voting such as voter identification laws, foreign and domestic disinformation, and other similar topics were outside the charge of the committee and, therefore, are not included in the report.

The Academies' report recommended that elections be conducted using human-readable paper ballots. It said that these ballots may be marked by hand or by machine using a ballot-marking device and that they may be counted by hand or by machine using an optical scanner.

The report further recommended that recounts and audits should be conducted by human inspection of the human-readable portion of the paper ballots and that voting machines that do not provide the capacity for independent auditing—for example, machines that do not produce voter-verifiable paper audit trails—should be removed from service as soon as possible.

Currently, there's no known way to secure a digital ballot. At this time, any election that does not employ paper ballots cannot be secure. Therefore, the report recommended that internet voting and specifically the electronic return of marked ballots should not be used at this time.

The Academies' report also recommended that vendors and election officials should be required to report any detected efforts to probe, tamper with, or interfere with election systems, including voter registration systems. Each State should require a comprehensive system of post-election audits of processes and outcomes. A detailed set of cybersecurity best practices for State and local election officials should be continuously developed and maintained. Congress should provide funding to help State and local governments modernize their election systems and improve cybersecurity capabilities.

Congress should authorize and provide funding for a major research initiative on voting. Recommendation 7.3 of the Academies' report says that "Congress should authorize and fund immediately a major initiative on voting that supports basic, applied, and translational research relevant to the administration, conduct, and performance of elections. This initiative should include academic centers to foster collaboration both across disciplines and with State and local election officials and industry."

This recommendation is bold, calls for research and development that provides solutions to issues identified in the report. I believe that a minimum of $25 million in funding over a five -year period would be needed to establish a national center.

As a Nation, we have the capacity to build an election system for the future, but doing so requires focused attention from citizens, Federal, State, and local governments, election administrators, and innovators in academia and industry. It also requires a commitment of appropriate resources.

Representative democracy only works if all eligible citizens can participate in elections and be confident that their ballots have been accurately cast, counted, and then tabulated.

Thank you for the opportunity to be here.

[The statement of Mr. Gilbert follows:]

UF | UNIVERSITY *of* FLORIDA

Herbert Wertheim College of Engineering
Computer & Information Science & Engineering

E301 CSE Building
PO Box 116120
Gainesville, FL 32611-6120
352-392.1200 Voice
352-392-1220 Fax

Chairperson Lofgren, Ranking Member Davis, members of the Committee,

I am honored to share with you my expertise in voting systems security, accessibility and usability. Let me begin by speaking about my background as it relates to this important topic. I am the Andrew Banks Family Preeminence Endowed Professor and Chair of the Computer & Information Science & Engineering Department at the University of Florida where I lead the Human Experience Research Lab. I have worked in elections for more than 15 years conducting research, developing innovative technologies and conducting studies with various elections stakeholders. In 2003, I developed an open source voting system called Prime III in response to the 2000 Presidential Election and the Help America Vote Act, or HAVA. To my knowledge, I am the only person to create an open source voting system that has been used in federal, state and local elections. Prime III was the first universally designed voting system, to my knowledge, meaning it was designed for all voters, independent of their ability or disability. The idea was one machine that everyone could use. This has benefits for accessibility, security and usability for voters and election administrators. For example, the margin of victory of the 2016 Presidential Election was smaller than the number of voters with disabilities that voted. If voters with disabilities are the only people voting using a specific type of technology, then adversaries could simply target that single population and impact the outcome of the election, see data from Rutgers' reports below. After HAVA was passed, each voting precinct was required to have at least 1 accessible voting machine. Although this was a good idea making progress towards increasing accessibility of our elections, there was one side effect. It setup a separate but equal experience for voters with disabilities. As such, there were unexpected issues introduced. For example, in some precincts, there were reports of the accessible voting equipment not being setup because the poll workers didn't know how to set it up. Essentially, because few voters used it, it was not something the poll workers gave much attention. Prime III has been used statewide in New Hampshire. New Hampshire adopted Prime III as their accessible voting machine and renamed it, One4All. Butler county, Ohio, which is my birth county, adopted Prime III as their remote accessible, absentee voting system in 2018. ES&S is the nation's largest voting machine manufacturer. ES&S created a machine called the Universal ExpressVote. ExpressVote was designed after Prime III. Dominion has the ImageCast Prime X machine that is very similar to Prime III as well. The research and development of Prime III was supported by the National Science Foundation and the U.S. Election Assistance Commission. The U.S. EAC supported this research and development through a 5 year accessible voting technologies grant that created the Research Alliance for Accessible Voting, RAAV. This grant helped setup Prime III research, development and studies that have resulted in improvement in the state of the art in elections technology. It also supported research and training for election administrators. Grants such as the EAC accessible voting technologies project are crucial to achieving the necessary security, accessibility and usability in our elections. Grants from the U.S. EAC have resulted in very good findings that are improving our elections.

I would like to transition now into specific recommendations. In 2018, the National Academies of Science, Engineering and Medicine released a consensus report titled, "Securing the Vote: Protecting American Democracy" The report was the result of a 2 year study conducted by experts from elections administration and policy, cybersecurity, accessibility, and law. I was a member of this committee. Over the course of the study, the committee reviewed extensive background materials. It held five meetings where invited experts spoke to the committee about a range of topics including voter registration, voting accessibility, voting technologies and market impediments to technological innovation, cybersecurity, post-election audits, and the education and training of election workers. The committee did not access classified information but instead relied on information in the public domain, including state and federal government reports, published academic literature, testimony from congressional hearings, and presentations to the committee. Issues related to voting such as voter identification laws, gerrymandering, foreign and domestic disinformation, campaign financing, and other similar topics were outside the charge of the committee and therefore, are not included in the report.

The committee was inspired by dedicated and enlightened election officials from across the nation and all levels of government. Such individuals are working tirelessly to improve accessibility, harness new technologies, and ensure the integrity of the results of elections. Unfortunately, these same officials often lack appropriate staff and resources and are routinely hampered in their work by a patchwork of laws and regulations that make it difficult to upgrade and modernize their election systems. U.S. elections are subject to aging equipment, targeting by external actors, a lack of sustained funding, and growing expectations that voting should be more accessible, convenient, and secure. The present issues and threat environment provide an extraordinary opportunity to marshal science and technology to create more resilient and adaptive election systems that are accessible, reliable, verifiable, and secure.

The Academies' study committee recognized that the federal government has an important role to play in understanding the impact of technological changes on the conduct of elections and in evaluating possible remedies to election threats. It noted that the U.S. EAC has a vital role to play in improving election administration and that NIST and NSF also have important roles to play in advancing the state of the art in US elections. The committee stated that the designation by the U.S. Department of Homeland Security of election systems as a subsector of the existing government facilities critical infrastructure sector is correct and appropriate, and that this designation reflects appropriately the need for sophisticated technical expertise and sharing of intelligence information required to protect the nation's election infrastructure.

We must foster an environment that promotes innovation in election systems technology, provides election administrators with human resource tools to increase the professionalization of the election workforce, allocates appropriate resources for the operation of elections, and better secures elections by developing auditing tools that provide assurances that ballots cast are counted and tabulated correctly and that the results of elections are accurate.

I would like to share some key recommendations from the report with you.

Elections should be conducted with human-readable paper ballots. These may be marked by hand or by machine, using a ballot-marking device; they may be counted by hand or by machine, using an optical scanner. Recounts and audits should be conducted by human inspection of the human-readable portion of the paper ballots. Voting machines that do not provide the capacity for independent auditing, for example, machines that do not produce a voter-verifiable paper audit trail, should be removed from service as soon as possible. Currently, there's no known way to secure a digital ballot. At this time, any election that is paperless is not secure. Therefore, Internet voting, specifically, the return of ballots should not be used at this time.

Vendors and election officials should be required to report any detected efforts to probe, tamper with, or interfere with any election systems, including, voter registration systems.

Each state should require a comprehensive system of post-election audits of processes and outcomes.

A detailed set of cybersecurity best practices for state and local election officials should be continuously developed and maintained.

Congress should provide funding to help state and local governments modernize their election systems and improve their cybersecurity capabilities. Congress should also authorize and provide funding for a major research initiative on voting. In the report, recommendation 7.3 says,

"Congress should authorize and fund immediately a major initiative on voting that supports basic, applied, and translational research relevant to the administration, conduct, and performance of elections. This initiative should include academic centers to foster collaboration both across disciplines and with state and local election officials and industry."

This recommendation calls for a bold initiative to foster research and development towards the mitigation of the issues outlined in the report. Such an initiative would be managed by the relevant existing government agencies. These agencies are the U.S. EAC, NIST, U.S. Department of Homeland Security, National Science Foundation, and U.S. Department of Defense (DoD). This initiative would call for a minimum of $25 million in funding over a 5-year period to establish a national center that has the primary focus of research and development as it relates to making all aspects of elections secure, accessible, usable and trustworthy. The center would work across universities, election officials, and elections technologies companies. The proposed research center is critical to protecting our elections and advancing the state of the art in elections to mitigate all domestic and foreign threats.

I would like to speak to a recent debate in the academic research community with respect to hand-marked paper ballots and ballot marking devices (BMD). As previously mentioned, in "Securing the Vote: Protecting American Democracy," the committee was clear in their recommendation that "Elections should be conducted with human-readable paper ballots. These may be marked by hand or by machine, such as a ballot marking device (BMD)." Following the release of the report, many States are moving away from paperless voting machines to hand-marked paper ballots or BMD. At the onset, it is important for voters to understand the difference in voting processes and how their votes are cast and counted.

In most BMD implementations, the voter makes selections using the BMD and a paper ballot is produced with a QR code or some other barcode and the voters' selections. The barcode(s) represent the voters' selections and are read by a separate scanner. In this case, some are concerned that the barcode may not match the human-readable portion of the ballot. To ensure a match, the national academies report recommends that all elections should undergo an audit, for example a risk-limiting audit (RLA). This recommendation also applies to hand-marked paper ballots as well because they are fed through a scanner for tallying. The audit would ensure that the election results are accurate and would neutralize any barcode mismatches. Furthermore, if the barcodes don't match, this provides a forensic trail to investigate the mismatch.

Hand-marked paper ballots, unlike BMD voting, are susceptible to overvoting and undervoting hacks. The undervote hack occurs when a voter decides not to make a selection in a contest, in other words, they leave the contest blank. This is a natural response when a voter doesn't want to vote for any candidates in a particular contest. An insider could then make a selection on that ballot. This will take two-to-five seconds and it's impossible to detect if the insider is not caught in the act. The overvote hack occurs when the voter makes a selection, but the insider makes an additional selection causing an overvote, which would lead to a nullified ballot. Like the undervote hack, this is undetectable unless the insider is caught in the act. These hacks require very little expertise and time.

There have been claims that voters do not review their ballots that have been produced by a BMD. Therefore, it's possible to flip votes so that what is printed on the ballot isn't what the voter selected and if the voter doesn't verify the ballot, the hack is successful. Dr. Michael Byrne at Rice University has just completed a study and his findings differ. Dr. Byrne and his colleagues have recently completed two separate studies on BMD ballot verification. One was a proper experiment and one was a field study in Los Angeles, California. For the experiment, they found that giving voters explicit reminders to verify their ballots resulted in a significant increase in verification rate. They also found a higher verification rate for a shorter ballot (5 races) than a longer one (40 races). Their results suggest that it is likely possible to improve verification rates with a little bit of instruction.

For the field study, they went out to Los Angeles to observe their mock election using their new VSAP (voting solution for all people) BMD, and found that 51% of voters verified (or appeared to verify) their printed ballots, and those that did took over 2 minutes longer to vote, which is presumably the verification time. This is a much higher verification rate than has been seen in some other studies, which is particularly surprising given that it was a mock election with nothing on the line for the voters.

My research lab has been working on a new voting machine interface that will further advance voter verification of paper ballots produced by BMD. We will begin to run studies of this new technology in February 2020. I would be happy to report our findings to you in the spring.

In my opinion, the gold standard for securing elections should be the audit. If necessary, a full manual recount should be possible. With this in mind, the BMD has an advantage over hand-marked paper ballots. Hand-marked paper ballots will suffer from ambiguous marks that are left to the auditors to interpret. This doesn't happen with the BMD. Some may say that the number of ballots that have this issue are small, but we have seen margins of victory very small, even down to one vote. Most importantly, every vote should count and every ballot should be auditable.

Lastly, I would like to emphasize the fact that there is no current technology to secure a digital ballot. Some have suggested that ballot encryption is a safe method to secure the ballot. This is not true. An encrypted ballot protects against modification, which is a common threat model in voting system security. In other words, the common threat has been that a bad actor would change votes in favor of their preferred candidate. An additional threat that is often ignored is chaos. Instead of tipping the election in favor of a specific candidate, the goal is chaos. In this scenario, encrypted ballots are extremely vulnerable. The hack would be to simply delete all the encrypted ballots. Essentially, this would nullify the election because all ballots would be lost. Another hack would be to hold the encrypted ballots for ransom with ransomware. In either case, the result is chaos and will cause doubt in the election results. Therefore, it is important to understand that no electronic ballot, including encrypted ballots, are secure at this time.

As a nation, we have the capacity to build an elections system for the future, but doing so requires focused attention from citizens, federal, state, and local governments, election administrators, and innovators in academia and industry. It also requires a commitment of appropriate resources. Representative democracy only works if all eligible citizens can participate in elections, have their ballots accurately cast, counted, and tabulated, and be confident that their ballots have been accurately cast, counted, and tabulated.

Sincerely, Juan E. Gilbert

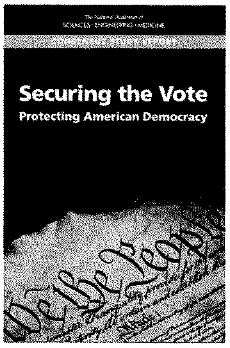
Juan E. Gilbert, Ph.D.
Andrew Banks Family Preeminence Endowed Professor & Chair
Computer & Information Science & Engineering Department (CISE)
Herbert Wertheim College of Engineering
University of Florida
P.O. Box 116120, Gainesville, FL 32611
[redacted]

Consensus Study Report

SEPTEMBER 2018 HIGHLIGHTS FOR FEDERAL POLICY MAKERS

SECURING THE VOTE

Protecting American Democracy


The National Academies of
SCIENCES · ENGINEERING · MEDICINE
CONSENSUS STUDY REPORT
Securing the Vote
Protecting American Democracy

The 2016 presidential election made clear the vulnerability of America's election infrastructure to foreign cyberattacks. Such attacks represent a new threat to the nation's system of representative democracy. A new report from the National Academies of Sciences, Engineering, and Medicine recommends concerted action by Congress, federal agencies, and state and local governments to protect the security and integrity of U.S. elections.

Securing the Vote: Protecting American Democracy recommends that focused attention be directed at strengthening cybersecurity for election systems. In addition, the report recommends that all U.S. elections be conducted with human-readable paper ballots by the 2020 presidential election. Risk-limiting audits should be implemented for all federal and state elections within a decade. And election systems should continue to be considered as U.S. Department of Homeland Security (DHS)-designated critical infrastructure. In addition, the report states that Internet voting should not be used for the return of marked ballots at the present time, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.

STEPS FEDERAL POLICYMAKERS SHOULD TAKE TO SECURE U.S. ELECTIONS

The report recommends that Congress:

- provide funding for state and local governments to improve their cybersecurity capabilities on an ongoing basis;
- create incentive programs for public-private partnerships to develop modern election technology; and
- authorize and fund immediately a major initiative on voting that supports research relevant to the administration, conduct, and performance of elections. This initiative should include academic centers to foster collaboration both across disciplines and with state and local election officials and industry.

The U.S. Election Assistance Commission (EAC) has a vital role to play in improving election administration, the report says. It urges the president to nominate and Congress to confirm a full commission and to ensure that the commission has sufficient members to sustain a quorum.

The National Academies of
SCIENCES · ENGINEERING · MEDICINE

The report also recommends steps Congress should take to support the EAC's work, including:

- appropriating funds for distribution by the EAC for the ongoing modernization of election systems;
- authorizing and funding the EAC to develop voluntary certification standards for voter registration databases, electronic pollbooks, chain-of-custody procedures, and auditing;
- providing the funding necessary to sustain the EAC's Voluntary Funding System Guidelines standard-setting process and certification program;
- requiring state and local election officials to provide the EAC with data on voting system failures and information on other difficulties arising during elections (for example, long lines, fraudulent voting, intrusions into voter registration databases); this information should be made publicly available; and
- fully funding the EAC to carry out its existing functions, as well as additional ones articulated in the report. For example, the report recommends that the EAC and DHS continue to develop and maintain a detailed set of cybersecurity best practices for state and local election officials. And it urges the EAC to closely monitor the expenditure of federal funds made available to states for the purposes of enhancing election security.

The report also recommends that Congress take steps to support work by the National Institutes of Standards and Technology (NIST) around election systems, including:

- authorizing and appropriating funds to NIST to establish Common Data Formats for auditing, voter registration, and other election systems;
- authorizing and providing appropriate funding to NIST to carry out its current elections-related functions and to perform the additional functions articulated in the report; and
- authorizing and funding NIST, in consultation with the EAC, to develop security standards and verification and validation protocols for electronic pollbooks, in addition to those standards and protocols developed for voting systems.

COMMITTEE ON THE FUTURE OF VOTING: ACCESSIBLE, RELIABLE, VERIFIABLE TECHNOLOGY

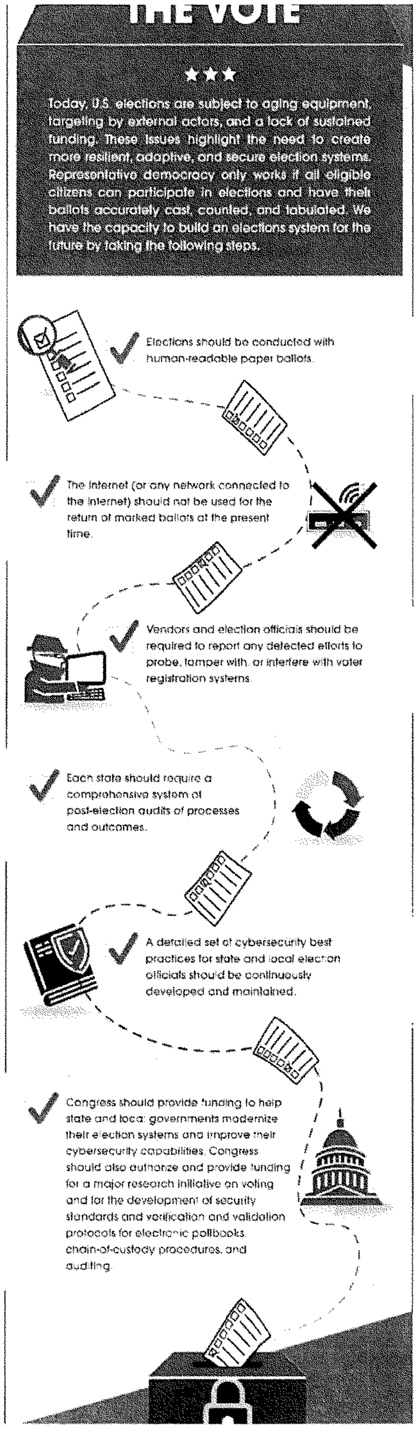
LEE C. BOLLINGER (Co-Chair), Columbia University; **MICHAEL A. McROBBIE** (Co-Chair), Indiana University; **ANDREW W. APPEL**, Princeton University; **JOSH BENALOH**, Microsoft Research; **KAREN COOK** (NAS), Stanford University; **DANA DeBEAUVOIR**, County of Travis, TX; **MOON DUCHIN**, Tufts University; **JUAN E. GILBERT**, University of Florida; **SUSAN L. GRAHAM** (NAE), University of California, Berkeley; **NEAL KELLEY**, County of Orange, CA; **KEVIN J. KENNEDY**, Wisconsin Government Accountability Board; **NATHANIEL PERSILY**, Stanford Law School; **RONALD RIVEST** (NAS/NAE), Massachusetts Institute of Technology; **CHARLES STEWART III**, Massachusetts Institute of Technology; Staff: **ANNE-MARIE MAZZA**, Study Director and Senior Director, Committee on Science, Technology, and Law (CSTL); **JON EISENBERG**, Senior Director, Computer Science and Telecommunications Board; **STEVEN KENDALL**, Program Officer, CSTL; **KAROLINA KONARZEWSKA**, Program Coordinator, CSTL; **WILLIAM J. SKANE**, Consultant Writer; **CLARA SAVAGE**, Financial Officer, CSTL.

For More Information . . . This Consensus Study Report Highlights was prepared by the National Academies of Sciences, Engineering, and Medicine based on the Report *Securing the Vote: Protecting American Democracy* (2018). The study was sponsored by the Carnegie Corporation of New York and the William and Flora Hewlett Foundation. Any opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of any organization or agency that provided support for the project. Copies of the Report are available from the National Academies Press, (800) 624-6242; http://www.nap.edu or at www.nationalacademies.org/futureofvoting.

Committee on Science Technology and Law
Policy and Global Affairs

The National Academies of
SCIENCES · ENGINEERING · MEDICINE

The nation turns to the National Academies of Sciences, Engineering, and Medicine for independent, objective advice on issues that affect people's lives worldwide.
www.national-academies.org



THE VOTE

★★★

Today, U.S. elections are subject to aging equipment, targeting by external actors, and a lack of sustained funding. These issues highlight the need to create more resilient, adaptive, and secure election systems. Representative democracy only works if all eligible citizens can participate in elections and have their ballots accurately cast, counted, and tabulated. We have the capacity to build an elections system for the future by taking the following steps.

✓ Elections should be conducted with human-readable paper ballots.

✓ The Internet (or any network connected to the Internet) should not be used for the return of marked ballots at the present time.

✓ Vendors and election officials should be required to report any detected efforts to probe, tamper with, or interfere with voter registration systems.

✓ Each state should require a comprehensive system of post-election audits of processes and outcomes.

✓ A detailed set of cybersecurity best practices for state and local election officials should be continuously developed and maintained.

✓ Congress should provide funding to help state and local governments modernize their election systems and improve their cybersecurity capabilities. Congress should also authorize and provide funding for a major research initiative on voting and for the development of security standards and verification and validation protocols for electronic pollbooks, chain-of-custody procedures, and auditing.

RUTGERS
School of Management
and Labor Relations

Fact sheet: Disability and Voter Turnout in the 2016 Elections

Lisa Schur and Douglas Kruse[1]

Key points:

- 16.0 million people with disabilities reported voting in the November 2016 elections.

- The voter turnout rate of people with disabilities was 6 percentage points lower than that of people without disabilities.

- Employed people with disabilities, however, were just as likely as employed people without disabilities to vote, suggesting that employment helps bring people with disabilities into mainstream political life.

- The voter registration rate of people with disabilities was 2 percentage points lower than that of people without disabilities. The lower voter turnout was due both to a lower registration rate among people with disabilities, and to lower turnout among those who are registered.

- If people with disabilities voted at the same rate as people without disabilities who have the same demographic characteristics, there would be about 2.2 million more voters.

These figures are based on analysis of data from the federal government's Current Population Survey Voting Supplement for November 2016. The computations were made using six disability questions introduced on the Current Population Survey in 2008.

Voter turnout among voting eligible population

		Millions who reported:	
	Percent voting	Voting	Not voting
Overall	61.4%	137.5	86.5
People without disabilities	62.2%	121.5	73.9
People with disabilities	55.9%	16.0	12.6
Hearing impairment	62.7%	5.1	3.0
Visual impairment	53.7%	2.1	1.8
Mental or cognitive impairment	43.5%	4.0	5.2
Difficulty walking or climbing stairs	55.9%	9.7	7.7
Difficulty dressing or bathing	44.6%	2.3	2.8
Difficulty going outside alone	44.7%	4.5	5.6

[1] Professors at the School of Management and Labor Relations, Rutgers University, 50 Labor Center Way, New Brunswick, NJ, 08901, Lschur@smlr.rutgers.edu and Dkruse@smlr.rutgers.edu.

As shown above, among the voting eligible population (citizens age 18 or older), 55.9% of people with disabilities reported voting, compared to 62.2% of people without disabilities. Within the disability population, the voting rate among people with hearing impairments (62.7%) was higher than the overall voting rate for people without disabilities, and the lowest rate was among those with a mental or cognitive impairment (43.5%). For each disability group except those with hearing impairments, the difference in turnout from those without disabilities is strong enough to be outside the survey's margin of error.[2]

The total of 137.5 million people who reported voting estimated from this survey is close to the total of 138.8 million ballots counted.[3] Any misreporting is unlikely to differ between the disability and non-disability populations, so the estimate of the turnout gap should be unbiased.

Some of the gap may be due to other demographic differences between people with and without disabilities. When adjusted for gender, race, age, education, and state of residence, the estimated gap expands slightly from 6.3 points to 7.8 points. This implies that if people with disabilities voted at the same rate as otherwise-similar people without disabilities, there would be an additional 2.2 million voters.

The estimated total of 16.0 million voters with disabilities compares with an estimated 17.1 million African-Americans and 12.7 million Hispanics/Latinos who voted in November 2016, based on analysis of this voting supplement. It should be noted that the disability total may be understated because these disability measures may not capture several types of disability.[4]

Some of the lower turnout of people with disabilities can be tied to difficulties getting to or using polling places.[5] A variety of states and localities have made efforts to reduce barriers and increase turnout among people with disabilities.[6] In addition, prior research has found the lower turnout is partly explained by lower levels of income, lower levels of political recruitment, and lower feelings of political efficacy.[7]

[2] The margins of error are based on a 95% level of confidence.

[3] http://www.electproject.org/2016g, accessed 5-22-17

[4] The disability questions measure the major sensory, mobility, and mental impairments, but may miss some learning disabilities and physical conditions that do not necessarily limit mobility, such as epilepsy and cancer.

[5] The Government Accountability Office released a report on June 10, 2009 finding that only 27% of polling places in 2008 had no potential impediments to access by people with disabilities, which was an improvement over 2000 when only 16% had no potential impediments (GAO-09-685). A 2012 household survey found that 30% of citizens with disabilities who had voted at a polling place in 2012 said they encountered difficulties in doing so, compared to only 8% of citizens without disabilities (Lisa Schur, Meera Adya, and Douglas Kruse, "Disability, Voter Turnout, and Voting Difficulties in the 2012 Elections," July 2013, http://smlr.rutgers.edu/sites/smlr.rutgers.edu/files/images/Disability%20and%20voting%20survey%20report%20for%202012%20elections.pdf).

[6] Lisa Schur, Meera Adya, and Mason Ameri. "Accessible Democracy: Reducing Voting Obstacles for People with Disabilities." Election Law Journal Vol. 14, No. 1, 2015, pp. 60-65.

[7] The prior findings are summarized in Lisa Schur, Todd Shields, and Kay Schriner, "Voting," in Gary Albrecht, ed., Encyclopedia of Disability (Thousand Oaks, CA: Sage Publications, 2005), and Lisa

Disability and voter turnout in 2008, 2012, and 2016

	2008	2012	2016
People without disabilities	64.5%	62.5%	62.2%
People with disabilities	57.3%	56.8%	55.9%
Disability turnout gap	-7.2%	-5.7%	-6.3%
Hearing impairment	63.1%	63.2%	62.7%
Visual impairment	56.8%	57.3%	53.7%
Mental or cognitive impairment	46.1%	44.8%	43.5%
Difficulty walking or climbing stairs	56.8%	56.3%	55.8%
Difficulty dressing or bathing	46.4%	46.7%	44.5%
Difficulty going outside alone	45.7%	47.3%	44.7%

These results can be directly compared to the general elections in November 2008 and 2012. As can be seen above, overall turnout dropped slightly from 2008 to 2012 and 2016. The drop was slightly greater for people without disabilities from 2008 to 2012, leading to a narrowing of the disability gap from 7.2 to 5.7 points, but the disability gap widened slightly to 6.3 points in 2016. It is important to note, however, that these estimated changes in the disability gap are small enough that they are within the survey's margin of error, so we cannot be confident of a true change in the disability gap over this period.

These results cannot be directly compared to elections before 2008 because they are based on a measure of disability introduced by the Census Bureau in 2008. A national survey conducted by the Eagleton Institute of Rutgers University following the November 2000 elections is comparable because it had similar questions and estimated prevalence of disability. Based on that survey, there was a 12 percentage point gap in voter turnout between people with and without disabilities in 2000, indicating that the relative voter turnout of people with disabilities in general elections may have improved from 2000 to 2016 (perhaps due in part to increased accessibility of polling places).[8]

Schur and Meera Adya, "Sidelined or Mainstreamed? Political Participation and Attitudes of People with Disabilities in the United States, Social Science Quarterly, Vol. 94, No. 3, 2013, pp. 811-839.

[8] Based on data used in Lisa Schur, Todd Shields, and Kay Schriner, "Generational Cohorts, Group Membership, and Political Participation by People with Disabilities," Political Research Quarterly, Vol. 58, No. 3, September 2005. Surveys conducted by Louis Harris and Associates for the National Organization on Disability show disability turnout gaps of 0% to 17% over the 1992-2008 period, but the disability prevalence is not reported so it is unclear if the disability measure used in those surveys can be readily compared (*The ADA, 20 Years Later: KesslerFoundation/NOD Survey of Americans with Disabilities*, Harris Interactive, New York, NY, 2010).

Breakdown by employment status and demographics

There was no gap in voter turnout between employed people with and without disabilities, indicating that employment helps provide resources and social contact that encourage voting.[9] The disability voting gap was concentrated among the non-employed, as shown in the numbers below. The disability gap was also:

- larger among women than among men, reflecting especially high voter turnout among women without disabilities;
- larger among white non-Hispanics than among other race and ethnicity groups
- larger among those age 18-34 and 35-49 than among other age groups
- largest in the Northeast and smallest in the West

Except for the comparisons among the employed and other race/ethnicity, each of these disability gaps is strong enough to be outside the survey's margin of error.

	Disability		No Disability		Disability Gap	
	2012	2016	2012	2016	2012	2016
Overall	56.8%	55.9%	62.5%	62.2%	-5.7%	-6.3%
Employed	64.6%	64.7%	64.2%	63.6%	0.4%	1.1%
Not employed	55.0%	54.0%	59.2%	59.2%	-4.2%	-5.2%
Women	56.5%	56.4%	64.8%	64.3%	-8.3%	-7.9%
Men	57.2%	55.4%	60.1%	59.9%	-2.9%	-4.5%
White non-Hispanic	57.5%	58.2%	65.2%	66.4%	-7.7%	-8.2%
African-American	62.8%	54.5%	67.2%	60.4%	-4.4%	-5.9%
Hispanic	46.8%	42.7%	48.1%	48.0%	-1.3%	-5.3%
Other race/ethnicity	47.5%	49.4%	50.2%	49.3%	-2.7%	-0.1%
Age 18-34	32.6%	33.1%	48.8%	49.7%	-16.2%	-16.5%
Age 35-49	45.4%	46.9%	63.5%	62.9%	-18.1%	-16.0%
Age 50-64	58.1%	54.5%	71.0%	69.2%	-12.9%	-14.7%
Age 65+	64.4%	63.9%	75.4%	73.8%	-11.0%	-9.9%
Northeast	54.5%	54.7%	63.3%	62.5%	-8.8%	-7.8%
Midwest	60.1%	58.7%	65.8%	65.2%	-5.7%	-6.5%
South	56.4%	54.1%	61.3%	60.9%	-4.9%	-6.8%
West	55.6%	57.3%	60.7%	61.1%	-5.1%	-3.8%

[9] This is consistent with other research on the role of employment summarized in Lisa Schur, Todd Shields, and Kay Schriner, "Voting," in Gary Albrecht, ed., Encyclopedia of Disability (Thousand Oaks, CA: Sage Publications, 2005)

Whether voted by mail and on election day

Among voters with disabilities in 2016, only 53% voted at the polling place on election day, compared to 61% of voters without disabilities. They were instead more likely to vote by mail before election day (28% compared to 19%), reflecting the mobility problems faced by some people with disabilities. All of these disability gaps are strong enough to be outside the survey's margin of error.

	Disability	No Disability	Disability Gap
How voted in 2016:			
At polling place on election day	52.6%	60.9%	-8.3%
At polling place before election day	18.1%	19.2%	-1.1%
By mail before election day	28.4%	18.6%	9.8%
By mail on election day	0.9%	1.4%	0.5%

State Breakdowns in Voter Turnout

The voter turnout gap between people with and without disabilities varied by state, as shown in the breakdown below. It should be cautioned that the sample size is low in many states, which increases the margin of error and decreases the likelihood of finding a disability gap that exceeds the margin of error. The disability gap in 2016 was large enough to be outside the margin of error (indicated by an "*") in 24 states and the District of Columbia, and was within the margin of error in the remaining 26 states.

	Disability		No Disability		Disability Gap			
	2012	2016	2012	2016	2012		2016	
U.S.	56.8%	55.9%	62.5%	62.2%	-5.7%		-6.3%	
Alabama	57.8%	47.4%	62.7%	59.4%	-4.9%		-12.0%	*
Alaska	59.1%	60.1%	58.3%	61.5%	0.9%		-1.5%	
Arizona	48.1%	66.2%	56.9%	59.6%	-8.9%		6.6%	
Arkansas	46.2%	51.2%	54.7%	60.1%	-8.4%	*	-8.9%	*
California	50.4%	52.3%	58.4%	58.6%	-8.0%	*	-6.3%	*
Colorado	65.6%	69.0%	71.1%	69.5%	-5.5%		-0.6%	
Connecticut	52.7%	65.0%	63.8%	63.8%	-11.1%	*	1.3%	
Delaware	71.1%	53.0%	66.8%	63.5%	4.3%		-10.5%	*
Florida	62.0%	58.9%	60.7%	59.5%	1.3%		-0.7%	
Georgia	54.9%	57.8%	62.9%	60.6%	-8.0%	*	-2.7%	
Hawaii	51.4%	54.1%	51.7%	46.3%	-0.2%		7.7%	
Idaho	56.6%	65.1%	64.9%	61.6%	-8.3%		3.5%	
Illinois	60.4%	65.8%	61.6%	63.5%	-1.2%		2.3%	
Indiana	54.8%	49.4%	59.9%	59.7%	-5.2%		-10.3%	*

Iowa	63.9%	56.1%	70.2%	64.7%	-6.3%		-8.6%	*
Kansas	63.0%	53.0%	63.3%	62.9%	-0.3%		-9.9%	*
Kentucky	48.5%	42.5%	61.4%	60.2%	-12.9%	*	-17.6%	*
Louisiana	58.7%	48.2%	67.6%	64.0%	-8.9%	*	-15.7%	*
Maine	55.9%	68.2%	71.0%	73.5%	-15.1%	*	-5.3%	
Maryland	58.3%	60.4%	66.0%	66.4%	-7.7%	*	-6.0%	
Massachusetts	59.7%	59.6%	72.3%	67.6%	-12.6%	*	-8.1%	*
Michigan	60.7%	63.7%	68.0%	64.4%	-7.3%	*	-0.7%	
Minnesota	65.7%	58.7%	74.2%	69.9%	-8.4%	*	-11.2%	*
Mississippi	67.9%	63.2%	75.9%	68.6%	-8.0%	*	-5.3%	
Missouri	53.5%	55.9%	65.8%	66.2%	-12.2%	*	-10.3%	*
Montana	64.9%	67.0%	65.8%	65.7%	-0.9%		1.3%	
Nebraska	62.2%	70.4%	61.5%	66.2%	0.7%		4.2%	
Nevada	58.5%	58.2%	57.9%	60.8%	0.7%		-2.6%	
New Hampshire	59.0%	66.0%	70.8%	69.4%	-11.9%	*	-3.4%	
New Jersey	56.8%	58.6%	62.5%	61.8%	-5.7%		-3.2%	
New Mexico	57.7%	54.4%	62.1%	54.9%	-4.5%		-0.4%	
New York	50.2%	48.8%	59.7%	58.4%	-9.5%	*	-9.6%	*
North Carolina	62.5%	64.5%	69.8%	68.0%	-7.3%	*	-3.5%	
North Dakota	57.2%	60.1%	64.7%	64.7%	-7.6%		-4.6%	
Ohio	58.3%	53.2%	63.9%	65.5%	-5.6%	*	-12.3%	*
Oklahoma	49.4%	51.7%	53.0%	57.6%	-3.6%		-5.9%	
Oregon	66.6%	53.9%	67.8%	68.8%	-1.1%		-14.9%	*
Pennsylvania	54.9%	54.1%	62.6%	64.0%	-7.7%	*	-9.9%	*
Rhode Island	61.0%	50.0%	62.7%	62.1%	-1.7%		-12.1%	*
South Carolina	59.8%	50.4%	65.5%	64.0%	-5.7%		-13.5%	*
South Dakota	64.7%	51.9%	60.4%	60.1%	4.2%		-8.1%	
Tennessee	47.9%	47.1%	57.4%	55.1%	-9.5%	*	-8.0%	*
Texas	55.8%	51.5%	53.5%	55.9%	2.3%		-4.4%	*
Utah	59.8%	63.3%	56.7%	62.6%	3.1%		0.7%	
Vermont	62.1%	57.6%	63.4%	63.2%	-1.3%		-5.6%	
Virginia	57.1%	57.4%	68.2%	69.5%	-11.1%	*	-12.0%	*
Washington	63.6%	62.5%	66.0%	66.8%	-2.4%		-4.4%	
Washington, D.C.	63.8%	60.0%	77.6%	76.1%	-13.8%	*	-16.1%	*
West Virginia	42.9%	45.9%	48.8%	52.0%	-5.8%		-6.1%	*
Wisconsin	66.5%	63.9%	74.7%	71.6%	-8.2%	*	-7.7%	*
Wyoming	59.7%	54.5%	58.7%	66.1%	1.0%		-11.6%	*

Voter Registration

The disability voting gap is due in part to lower voter registration, but is due more to a lower likelihood of voting if registered. Among people with disabilities, 68% were registered to vote, only 2 points lower than the rate for people without disabilities. Among those who were registered, 82% voted, which was 6 points lower than for registered people without disabilities. People with disabilities were more likely than those without disabilities to have registered at a town hall or registration office, public assistance agency, or registration drive, and less likely to have registered at a department of motor vehicles or using the Internet.

Each of these disability gaps is strong enough to be outside the survey's margin of error, except for the gaps in registering by mail or at a polling place.

	Disability	No Disability	Disability Gap
Registered to vote	68.3%	70.6%	-2.3%
Voted if registered	82.0%	88.0%	-6.0%
How registered to vote:			
Went to a town hall or county/ government registration office	28.5%	20.1%	8.4%
At a department of motor vehicles	24.8%	32.5%	-7.7%
At a public assistance agency	2.2%	1.2%	1.0%
Registered by mail	15.4%	15.1%	0.3%
Registered at polling place	7.6%	7.2%	0.5%
Filled out form at a registration drive	6.0%	4.7%	1.3%
At a school, hospital, or on campus	5.2%	6.4%	-1.2%
Registered using the Internet or online	4.0%	8.3%	-4.4%
Other	6.4%	4.5%	1.8%

Why people were not registered

The most common expressed reason for not registering to vote, among people both with and without disabilities, was a lack of interest in the election or politics. Almost one-fourth of people with disabilities (23%) gave "permanent illness or disability" as their reason for not being registered.

The disability gaps below are strong enough to be outside the survey's margin of error, except for the small disability gaps in "Not eligible to vote," "Did not know where or how to register," "Difficulty with English," and "Other reason."

If not registered to vote, why not:	Disability	No Disability	Disability Gap
Not interested in the election or not involved in politics	36.1%	45.3%	-9.3%
Permanent illness or disability	22.6%	1.6%	20.9%
Did not meet registration deadlines	6.7%	14.0%	-7.3%
Not eligible to vote	7.6%	7.8%	-0.3%
My vote would not make a difference	3.5%	5.4%	-1.9%
Did not know where or how to register	3.1%	3.5%	-0.4%
Did not meet residency requirements/did not live here long enough	1.3%	3.1%	-1.7%
Difficulty with English	2.4%	2.0%	0.5%
Other reason	16.8%	17.3%	-0.5%

Why people did not vote if registered

Among those who were registered to vote but did not do so in November 2016, about one-third (36%) of people with disabilities gave "illness or disability" as the reason for not voting, compared to 7% of people without disabilities. People with disabilities were also more likely to cite transportation problems as a reason for not voting (7% compared to 2%), consistent with their higher rate of voting by mail. They were less likely than people without disabilities to say that they were not interested, too busy, out of town, or didn't like the candidates.

The disability gaps below are strong enough to be outside the survey's margin of error, except for the small disability gaps in "Forgot to vote," "Bad weather conditions," "Registration problems," and "Other."

Why didn't vote	Disability	No Disability	Disability Gap
Illness or disability (own or family's)	35.7%	6.6%	29.0%
Not interested, felt my vote wouldn't make a difference	9.6%	17.3%	-7.6%
Didn't like candidates or campaign issues	20.6%	26.5%	-6.0%
Too busy, conflicting work or school schedule	4.4%	17.0%	-12.6%
Forgot to vote (or send in absentee ballot)	3.2%	3.1%	0.1%
Transportation problems	6.8%	1.8%	5.0%
Out of town or away from home	4.0%	9.1%	-5.1%
Registration problems (i.e. didn't receive absentee ballot, not registered in current location)	3.6%	4.7%	-1.1%
Inconvenient hours, polling place or hours or lines too long	1.4%	2.4%	-1.0%
Bad weather conditions	0.1%	0.0%	0.0%
Other	10.8%	11.6%	-0.8%

The CHAIRPERSON. Thank you very much.

Reverend Spearman, we'd love to hear from you.

TESTIMONY OF REV. T. ANTHONY SPEARMAN

Rev. SPEARMAN. Good afternoon, Chairperson Lofgren, Ranking Member Davis, and Committee Members.

I am indeed honored to be here, for, unlike the previous participants on these panels, I am neither a voting systems vendor nor an expert. I'm an activist, one who was raised in a household where the vote was held sacred.

I'm the president of the North Carolina State Conference of Branches of the National Association for the Advancement of Colored People and the only county board of elections member of color from Guilford County, North Carolina. And while not an expert in election security, I rely on the findings of those scientists who are and urge my colleagues on county boards across the Nation to do so as well. We must listen to scientists, not vendor marketing claims.

Dr. Alex Halderman just published research and finds that electronic ballot-marking devices do not create ballots that can be reasonably audited, which is consistent with the recently expanded study by Dr. Philip Stark, Dr. Richard DeMillo, and Dr. Andrew Appel concluding that electronic ballot-marking devices cannot be relied on to produce elections that assure the will of the people.

Dr. Duncan Buell, along with others, has studied how voting machines and their allocation can create lines that frustrate and disenfranchise voters.

Let me hasten to say that I am not anti-technology, but I agree with the scientists who argue that election security can be compromised by placing an electronic device between a voter and the ballot.

While the election security defenses needed to detect and stop cyber-attacks may seem impossibly complex and overwhelming, there's a practical, low-tech, traditional answer to mitigating the greatest threats, assuring that any attacks can be detected and cannot be ultimately achieved or effective.

That's where I come in. I was first elected to the Guilford County Board of Elections in 2017 for a two-year term and reelected in January 2019 for another two-year term. During my first term, I was the only member of the board without a legal degree. All I had sitting at the table with me was my activism, passion for voters, and my experience working in elections.

Prior to my election to a seat on the Guilford County board, my volunteerism as a precinct worker began as an election day specialist around 2017 in Catawba County after a growing number of members began venting their frustrations with the voting process.

Coincidentally, this was the same year that tremendous advances for voters occurred in the State of North Carolina. Same-day registration began allowing voters to cast ballots during the early-voting period, which led to an increase in voter participation during the November 8, 2008 Presidential election. In Catawba County, voters used hand-marked paper ballots.

In 2014, when I was appointed to a church in Greensboro, an opportunity to work at a precinct in Guilford County presented itself.

And there I worked as a judge and on to becoming the chief judge, or overseer, of FEN1, one of the largest precincts in the county.

In Guilford County, iVotronics, or direct recording electronics, DREs, were in use. And among my growing concerns while serving the precinct were problems that arose with the touch-screen or iVotronic devices.

I was the overseer, chief overseer, of the sixth-highest voter precinct in Guilford County, with 3,800 voters. As one of my friends has convinced me, the first line of defense is the local county bipartisan election board, like the one I sit on in Guilford County, North Carolina. Across the Nation, they are authorities for selecting voting systems and reviewing the ballot tabulations before they certify the election results.

If voters, campaigns, political parties, and candidates insist that these boards, one, select only hand-marked paper ballots as standard equipment; two, maintain ballot chain of custody; three, distribute an accurate paper backup pollbook to the polls; and, four, conduct vigorous reviews of the election returns and tabulations before certifying, cyber- attacks cannot be successful. They can't be prevented, but the jurisdiction can recover from them and verify the will of the people. I'm talking first line of defense.

As a first-time witness of the process for voting machine certification, I must admit I was highly disturbed that the demonstration was conducted in what I viewed as an inconvenient place, off the beaten path for most voters. As I drove to the site, I became overwhelmed with how un-user-friendly this location was for minorities, and, as I recall, I was the only person of color in attendance.

But not only that, when I reviewed the agenda and saw how the demonstration was to be conducted, with the majority of time allotted to county board members and only a few minutes left for the public to view systems, I immediately called the director of elections and expressed my displeasure with the setup. By the time I arrived, the necessary adjustments had been made, and everyone moved through the demonstrations together.

Elections belong to the people, and the more the people are included in the process, the more we may gain their trust and confidence.

Thank you for allowing me to share.

[The statement of Rev. Spearman follows:]

Reverend Dr. T. Anthony Spearman

Written Testimony

To the

Congress of the United States

House of Representatives

Committee on House Administration

January 9, 2020

I am the Reverend Dr. T. Anthony Spearman. I am an ordained elder in the African Methodist Episcopal Zion Church, the President of the North Carolina State Conference of Branches of the National Association for the Advancement of Colored People and a member on the Guilford County Board of Elections. I am honored to be here today, and although not a vendor or an expert, I hope that the testimony I offer on the election security question will help us move closer to "form a more Perfect Union, establish Justice, Insure domestic tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity" and shape, for generations to come, a newer and truer democracy than the one present to us today.

I was reared in a household where the right to vote was held sacred and I learned to exercise that right by voting in every election since my eighteenth year of existence. For nearly fifty years I have participated in Voter Registration Drives, Get Out the Vote efforts and while pastoring encouraged and led these endeavors at the church, going from door to door registering people to vote and most recently, in my role as President of the State Conference of Branches NAACP requesting the opportunity to get into the jails to register eligible voters. I am a staunch advocate of the 15th Amendment which states, "the right of citizens of the United States to vote shall not be denied or abridged by the United States or by any State on account of race, color, or previous condition of servitude. The Congress shall have power to enforce this article by appropriate legislation."

My experience as a Board of Elections precinct worker in the State of North Carolina began around 2007 in Catawba County after a growing number of church members began venting their frustrations with the voting process, which sounded a great deal like voter suppression but more importantly they had no one to voice their concerns. Coincidentally, this was the same year that Same Day Registration began in the state allowing voters to cast ballots during the early voting period (third Thursday before an election until the Saturday prior to Election Day) which led to an increase in voter participation during the November 2008 presidential election. There, in Catawba County, voters voted by hand marking their paper ballots and I was assigned to a precinct in the white community of Sherrill's Ford, where things usually ran smoothly. I began working as an Election Day Specialist (EDS) who managed all the questions of voters whose names did not appear on the books and directed them to the correct precinct or cleared the way for them to at least cast a provisional ballot. Then I worked my way through the ranks serving as an assistant, and judge.

It was around this time, post Shelby v. Holder (June 25, 2013 when the Supreme Court of the United States returned its' decision eviscerating Section 4 of the Voting Rights Act of 1965) that my activism for voting rights spiked and my perspicacity for voter suppression grew, resulting in increased attendance at Legislative sessions in Raleigh and County Board of Election meetings and staying abreast of voting laws enacted, which instantly increased after June 25, 2013, like the "monster" voter suppression law **House Bill 589; an act to restore confidence in government by establishing the voter information verification act to promote the electoral process through education and increased registration of voters and by requiring voters to provide photo identification before voting to protect the right of each registered voter to cast a secure vote with reasonable security measures that confirm voter identity as accurately as possible without restriction, and to further reform the election laws; the bill's short title was known as the Voter Information Verification Act or (VIVA).** The bill was introduced as a 14-page document but by the time of its ratification had mushroomed into a 64-page monstrosity that reduced the number of early voting days, did away with same day registration and pre-registration of 16-17-year olds and eliminated out of precinct voting. A rash of other bad bills that would have made it harder for a person to vote soon followed.

In 2014 when I was appointed to a church in Greensboro an opportunity to work in a precinct in Guilford County presented itself and there I worked as a judge and on to becoming the Chief Judge of FEN1, one of the largest African American precincts in the county. In Guilford County, iVotronics or direct-recording electronics (DREs) were in use and among my growing concerns while serving the precinct were problems that arose with the touch screen or iVotronic devices. Eventually, the opportunity arose to offer myself for a seat on the Guilford County Board of Elections.

I was first elected to the Guilford County Board of Elections in 2017 for a two-year term and reelected in January of 2019 for another two-year term. During my first term I was the only member without a legal degree and the only African American, but I sat at the table on that board with my experience of working in the precinct and passion for the voter.

Having had the opportunity to serve the public as a member of the Hickory Public School Board of Education I developed a discipline of being responsible and accountable to the people I served. There, rather than being overly concerned with always arriving at consensus as a board (for appearance sake) I learned to ask questions and vote my conscience. I am certain this was a by-product of my activist background and I resolved to take that same discipline on to the Guilford County Board of Elections.

On April 16, 2019 the NC NAACP legal team made a presentation entitled "The Fight Against Voter Suppression Continues." On April 18, 2019 the Mueller Report was released which I bought and read.

On May 21, 2019, Dr. Rodney Sadler, the Health Chair of the NC NAACP Executive Committee text to introduce me to a John Brakey, an election specialist and Executive Director of AUDIT

USA (Americans United for Democracy, Integrity and Transparency in Elections). He was in North Carolina examining our elections process. On Saturday, June 1, 2019, I invited John to join me during the Annual Conference of the West Central North Carolina Conference of the Piedmont Episcopal District of the African Methodist Episcopal Zion Church. There I serve as the Director of Voter Registration of the entire district covering three conferences.

From that day my knowledge of all aspects of elections began to increase and I became familiar with terms like Election Assistance Commission (EAC), Voluntary Voting Systems Guidelines (VVSG), cybersecurity and seeking to make elections transparent, trackable and publicly verifiable. Through Brakey, I started reading election law blogs and educating myself on the certification process. It seemed that the decertification of DREs was imminent and the certification of new machines was soon to occur, but then on June 24, 2019 I received a text stating that the NC General Assembly was planning to extend the use of DREs through the 2020 election. This would be the second time that their life had been extended after a bill passed in 2013 outlawing their use after 2018. It was then that I grew suspicious and turned to scrutinizing voting system vendors, especially Election Systems & Software (ES&S). It was also about this time that I learned of a $10 million dollar bond to keep other vendors out of North Carolina from bidding on new equipment. The $10 million would effectively mandate a single source for NC election machines, forcing all 100 counties to buy the same brand of equipment at non-competitive prices. This was not good democracy. Had Guilford County worked so long with ES&S equipment that they developed a bias which prevented the consideration of other vendors? I could not say but it sometimes appeared that many of the board decisions were relegated to the director or at least reliance on his "recommendations" without much discussion began to disturb me and I vocalized my concern and conducted research on my own.

This was about the time that legislative changes to absentee ballots began surfacing largely because of the election fraud discovered in North Carolina's Ninth Congressional District and I first met with Karen Brinson-Bell, the new Executive Director of the State Board of Elections at the Legislative Building. By the time our brief meeting ended, I sensed she was strongly biased toward the vendor, ES&S and was not open to talking with outside experts or specialists.

I became aware that ES&S employed six lobbyists and I knew one of them reasonably well. We talked. He shared concerns about the DREs and how they were banned in Florida in 2006 but he was a strong supporter of the expensive BMDs which I am not, mainly because of the bar codes they use, which I cannot read.

Some of the papers of experts like Professor Duncan Buell and Phillip Stark began to inform me about the dangers of these machines creating long lines and perpetuating voter suppression.

On Sunday July 28, 2019, the State Board of Elections held an open meeting. Convinced that the board intended to certify machines that night, many advocates of hand marked paper ballots filled the room.

That night the board voted 3-2 to delay certification until the next meeting. The chair resigned the next day.

On August 23, 2019, the meeting was held with the new Chair presiding and the vote to certify three vendors (ES&S, Hart InterCivic and Clear Ballot) carried 3-2.

Many of us reminded the State Board of

§163A-1115(e) ***"Prior to certifying a voting system, the State Board shall review, or designate an independent expert to review, all source code made available by the vendor pursuant to this section and certify only those voting systems compliant with State and federal law. At a minimum, the State Board's review shall include a review of security, application vulnerability, application code, wireless security, security policy and processes, security/policy program management, technology infrastructure and security controls, security organization and governance, and operational effectiveness, as applicable to that voting system. Any portion of the report containing specific information related to any trade secret as designated pursuant to G.S. 132-1.2 shall be confidential and shall be accessed only under the rules adopted pursuant to subdivision (9) of subsection (f) of this section. The State Board may hear and discuss the report of any such review under G.S. 143-318.11 (a)(1).***

Having met with a number of election specialists and experts the NC NAACP organized an emergency town hall meeting asking the question, "Who Shall Profit? Vendors or Voters." The Emergency Town Hall meeting was streamed in five locations, Charlotte, Raleigh, Fayetteville, Winston-Salem and Broadway, NC. We featured experts; among them Dr. Andrew Appel, and Professor Duncan Buell and we drew one County Board of Elections member, one State Board of Elections member and one Guilford County Commissioner.

After two postponements to vote on a system, Guilford County Board of Elections decided to proceed with Hand Marked Paper Ballots. Below is a list of the equipment we will purchase.

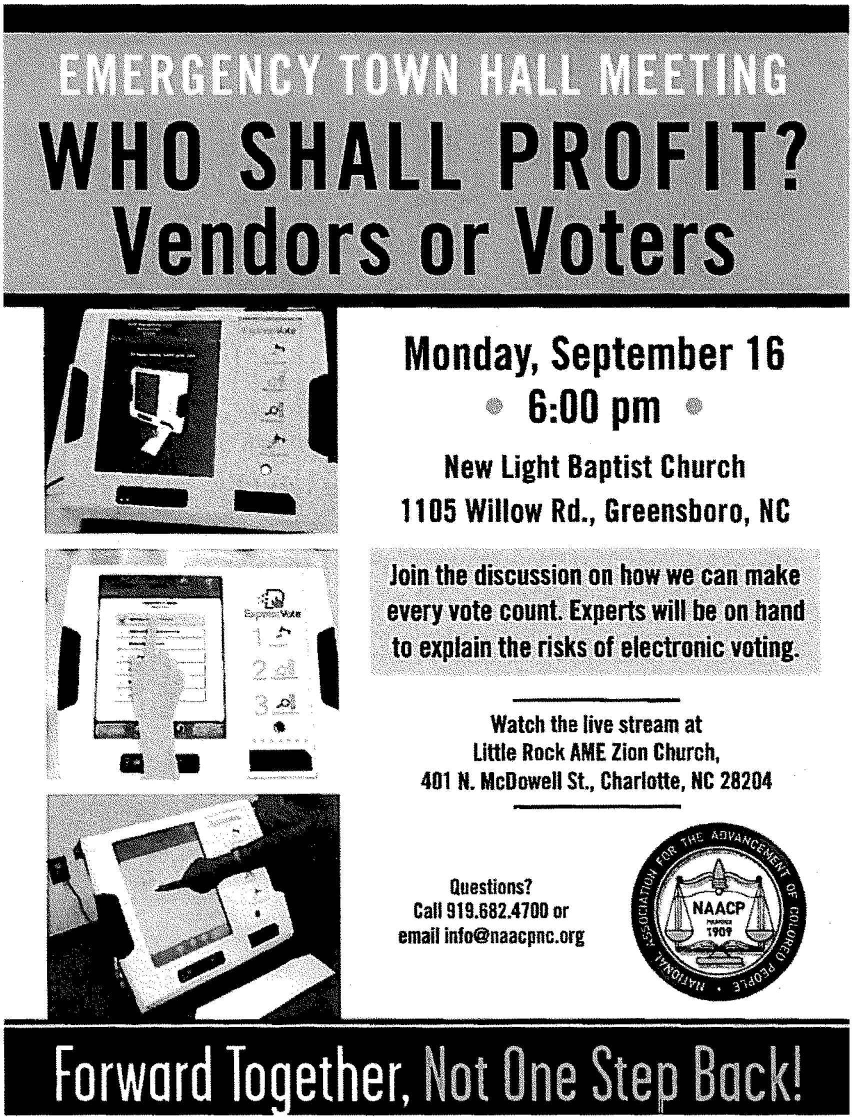
- For the polling places: **ES&S DS200** Digital Scanner with paper ballots
- Formula for this was one unit per voting site (165 precincts + 30 early voting sites + 25 spares).
- For ADA compliance: **ES&S AutoMark** Ballot Marking Device
- Formula for this was one unit per voting site (165 precincts + 30 early voting sites and no spares because they can be reallocated between the voting methods very easily).
- For High-Speed Central Scanning: **ES&S DS850 Digital** Scanner
- Formula for this was two units to expedite any large recounts and also to have one as a backup.
- As for booths, the county is buying enough nice folding booths with aluminum legs to equal the footprint of our current voting machines (about 1,400) and then buying another 800-1000 corrugated plastic privacy screens that will sit on table tops (folding tables, cafeteria tables, library tables, etc.).

- The software version is ElectionWare 5.2.2.0.

- Additionally, Guilford County will enter into a contract that allows us to code our own ballots – that is create and design our own paper ballots and program the units and tabulation software – without the vendor. Many counties rely on the vendor to program their elections, but Guilford County's Director and Assistant Director have been trained and are authorized to do our own.

The Guilford County Board of Commissioners had budgeted $8,000,000 for the voting system and our total cost came to $2,200,000 amounting to a savings of $5,800,000 which the commissioners partially reallocated to increase the pay of school bus drivers and other employees.

We would hope others would follow the Guilford County model. We remain reasonably assured that it will help to restore trust and confidence in the election process.



EMERGENCY TOWN HALL MEETING

WHO SHALL PROFIT? Vendors or Voters

Monday, September 16

• 6:00 pm •

New Light Baptist Church
1105 Willow Rd., Greensboro, NC

Join the discussion on how we can make every vote count. Experts will be on hand to explain the risks of electronic voting.

Watch the live stream at
Little Rock AME Zion Church,
401 N. McDowell St., Charlotte, NC 28204

Questions?
Call 919.682.4700 or
email info@naacpnc.org

NATIONAL ASSOCIATION FOR THE ADVANCEMENT OF COLORED PEOPLE • NAACP FOUNDED 1909

Forward Together, Not One Step Back!

The CHAIRPERSON. Thank you very much.

Commissioner Palmer.

TESTIMONY OF THE HONORABLE DONALD PALMER

Mr. PALMER. Good afternoon, Chairperson Lofgren, Ranking Member Davis, and Members of the Committee. I'm thankful for the opportunity to testify before you today on the important work being done by the United States Election Assistance Commission in preparation for the 2020 Federal elections.

As prescribed by the Commission's enabling legislation, the Help America Vote Act of 2002, HAVA, the EAC is focused on State and local election officials across the United States and providing secure, accessible, and accurate elections. Under that act, the EAC works to implement election reforms, assist States in certifying voting systems, advance voting accessibility, disburse HAVA funds, and serve as a clearinghouse of election information and best practices in the laboratory of States.

In pursuit of this mission, we collaborate closely with State and local election officials, Federal partners, and others in the election community.

I am grateful that the expert and vendor witnesses testifying before you today have shared their insight on the important topic of election security.

I would like to begin by thanking Congress for your recent efforts to increase funding in this area. The addition of $425 million in HAVA grant funds, with a 20-percent State match, will go a long way toward enhancing election technology and improving security in State and local elections.

Simultaneously, the 40-percent increase in the EAC budget will allow us to bolster existing programs and enhance resources. I should note that EAC's distribution of $380 million in 2018 HAVA funds to the States in the lead-up to the midterm elections was and continues to be, critically important to helping officials secure the elections infrastructure.

I would like to highlight an important update to our testing and certification program. The testing and certification program manual allowed for minor, de minimis changes, software changes, without the overhead of a full-blown voting system certification campaign. In November of 2019, the EAC's testing and certification program issued a notice of clarification, providing clear guidelines on submitting these minor changes for certification. The EAC expects that this process will be used by vendors to rapidly update the security of their systems with the latest software patches and operating system updates.

Tremendous progress was also made in 2019 toward the adoption of voluntary voting system guidelines, what we call VVSG 2.0. VVSG 2.0 will represent a significant leap forward in defining new standards that will serve as the template for the new generation of secure and accessible voting systems.

The hard work of NIST staff and EAC personnel culminated in the presentations of these draft requirements to the Technical Guidelines Development Committee. This committee is now considering the recommendations to the EAC on adoption.

My fellow commissioners and I are committed to a transparent and thorough deliberation on the path to implementing VVSG 2.0. The EAC Standards Board and the Board of Advisors will meet in April of 2020 to consider these new requirements, and after their key input, it is my hope that the VVSG 2.0 will be finalized and voted on in the upcoming months.

As the Nation focuses on the 2020 election this year, so does the EAC. On January 14, we are bringing together election officials and experts in election security and accessibility to kick off our #2020Focus campaign at the National Press Club. The topics for discussion will include the security environment, the need for enhanced poll-worker training, and ensuring accessible elections for all Americans.

The increased fiscal year 2020 appropriations for the EAC will allow us to fill critical staffing vacancies within the agency as well as bolstering our staff to meet rising demands. I am pleased to report that the EAC is in the process of identifying candidates for a new general counsel and additional communication personnel. The statutory process for identifying candidates for executive director is well underway.

We also plan to add staff in our testing and certification program. Expansions to this program will enhance the capability of handling frequent voting system security updates through the de minimis process while fulfilling its other duties of conducting training for election administrators, performing on-site audits of voting system manufacturing and test lab facilities, and overseeing a risk-limiting audit assistance program.

HAVA has set forth an ambitious agenda for the EAC, one rooted in protecting the very foundation of our Nation's democracy. Despite very real and persistent resource challenges in recent years, the EAC has fulfilled its obligation and even expanded the support it provides to election administrators and voters.

With strong support from the Congress in the recent appropriations cycle and the reestablishment of a quorum of commissioners, the EAC is ready for its next chapter. We look forward to working with the Congress as we continue our efforts to help America vote.

I am happy to answer any questions you may have following today's testimony.

[The statement of Mr. Palmer follows:]

U.S. Committee on House Administration
2020 Election Security - Perspectives from Voting System Vendors and Experts

Donald Palmer, Commissioner
United States Election Assistance Commission (EAC)
January 9, 2020

Good morning Chairperson Lofgren, Ranking Member Davis, and members of the committee. I'm thankful for the opportunity to testify before you this morning on the important work being done by the U.S. Election Assistance Commission (EAC) in preparation for the 2020 federal elections. As prescribed by the Commission's enabling legislation, the Help America Vote Act of 2002 (HAVA), the EAC is focused on assisting state and local election officials across the United States in providing secure, accessible, and accurate elections. Under that act, the EAC works to implement election reforms, assist states in certifying voting systems, advance voting accessibility, disperse HAVA funds, and serve as a clearinghouse of election information and best practices in the laboratory of states. In pursuit of this mission, we collaborate closely with state and local election officials, federal partners, and others in the elections community. I am grateful that the expert and vendor witnesses testifying before you today have shared their insight on the important topics of election security.

I would like to begin by thanking Congress for your recent efforts to increase funding in this area. The addition of $425 million in HAVA grant funds with a 20% state match will go a long way toward enhancing election technology and improving security in state and local elections. Simultaneously, the 40% increase in the EAC budget will allow us to bolster existing programs and enhance resources. I should note the EAC's distribution of $380 million in 2018 HAVA funds to states in the lead up to the 2018 midterms was, and continues to be, critically important to helping officials secure elections infrastructure.

Before discussing the hard work currently underway at the EAC, I would first like to highlight an important update to our Testing and Certification Program that occurred late last year. As the committee may already be aware, the Testing and Certification Program Manual allowed for minor – or de minimis – software changes without the overhead of a full-blown voting system certification testing campaign. Our goal is to be nimble as possible in working with manufacturers to quickly respond to a rapidly changing threat environment. While this procedure has existed for a number of years, it became clear during the Commission's public forum on Election Security last August that the guidelines and procedures around these changes were not clear to a number of key stakeholders in the community including vendors, testing laboratories, and state election officials performing state certification. So, in November of 2019, the EAC's Testing and Certification Program issued a Notice of Clarification providing clear guidelines on submitting these minor software changes for certification. The EAC expects that this process will be used often by vendors to rapidly update the security of their systems with the latest software patches and operating system updates.

Tremendous progress was also made in 2019 toward the adoption of Voluntary Voting System Guidelines (VVSG) 2.0. The VVSG 2.0 represents a significant leap forward in defining standards that will serve as the template for the next generation of secure and accessible voting systems. The hard work of the NIST staff, and EAC staff culminated in presentations of draft requirements to the Technical Guidelines Development Committee. The Committee is now considering their recommendations to the EAC on adoption. My fellow commissioners and I are committed to a transparent and thorough deliberation on the path to implementing VVSG 2.0. The EAC Standards Board and the Board of Advisors will meet in April 2020 to consider these new requirements. After their key input, it is my hope that the VVSG 2.0 will be finalized and voted on over the upcoming months.

As the nation focuses on the 2020 election this year, so too does the EAC. Our #2020Focus campaign kicks off with the 2020 Election Summit at the National Press Club next Tuesday, January 14th. The Summit will bring together election officials and experts in election security and accessibility. Topics for discussion include the security environment, the need for enhanced poll worker training, and ensuring accessible elections. Moving forward, we look forward to keeping you and the public informed through our website and Twitter feed. These will be updated throughout the year with new election administration information and best practices gathered from our partners and developed internally in our research, clearinghouse, and testing and certifications programs.

The increased fiscal year 2020 appropriations for the EAC will allow us to fill critical staffing vacancies within the agency as well as bolstering our staff to meet rising demands. I am pleased to report that the EAC is in the process of identifying candidates for a new General Counsel and additional communications personnel. The statutory process of identifying candidates for Executive Director is also well underway. The EAC plans to hire staff across the agency. Specifically, we also plan to add staff in our Testing and Certification Program. Expansions to this program will enhance its capability of handling frequent voting system security updates through the de minimis process while fulfilling its other duties of conducting training for election administrators, performing on-site audits of voting system manufacturing and test lab facilities, and overseeing a Risk-Limiting Audit assistance program.

As a former Naval Intelligence Officer, I understand the critical importance of establishing clear lines of communication and confidence in responding to advanced cyber threats. Election officials should not be forced to consult a rolodex of contacts when time is of the essence – they should have a trusted partner to call. The EAC is uniquely positioned as the only agency dedicated to serve in this role.

HAVA set forth an ambitious agenda for the EAC, one rooted in protecting the very foundation of our nation's democracy. Despite very real and persistent resource challenges in recent years, the EAC has faithfully fulfilled its obligations and even expanded the support it provides to election administrators and voters. With strong support from Congress in the recent appropriations cycle and the reestablishment of a quorum of Commissioners, the EAC is ready for its next chapter. We look forward to working with Congress as we continue our efforts to help America vote. I am happy to answer any questions you may have following today's testimony.

The CHAIRPERSON. Thank you very much.

And last but certainly not least, Mr. Gianasi.

TESTIMONY OF MIKE GIANASI

Mr. GIANASI. Thank you.

Chairperson Lofgren, Ranking Member Davis, and all the other honored Committee Members here today, thank you for the invitation to come and speak before you.

As stated previously, Ranking Member Davis and I are friends. We've grown up in the same town. It's in central Illinois. It's the town of Taylorville, which is the county seat of the county of Christian in Illinois. Also as stated previously, I was appointed as the county clerk and recorder in 2017 upon the retirement of that previous clerk and recorder. Subsequently, I was elected as the county clerk and recorder in 2018, of which I currently serve as today.

The introduction of my tenure as the election authority was rather swift and, at that time, being in the 2017–2018 timeframe, focused on an increase in cybersecurity-related responsibilities. I had not been a participant in this arena prior to that time period, so although there were a lot of discussions and a lot of other situations that had occurred previously, I was not a party to that. However, as the new election authority, it has become my responsibility to take into account all of these situations and, now, all of the increasing responsibilities as the days go by.

As the election authority, my primary concern on the topic of elections involves several categories, one being physical security of course. The election equipment that I have custody of is stored away in my courthouse in a locked room.

That election equipment, by the way—I might as well make this comment—is being delivered today because, as of recently, I have been approved the ability to obtain new election equipment. My previous election equipment was the AccuVote and TSx-type model equipment from Diebold, which is no longer being used by Christian County. We have now upgraded our equipment to the new equipment provided by Unisyn Voting Solutions, Incorporated, who is not here today.

In regards to meeting with my election vendor, who I have trusted for many, many years and previous clerks have trusted for many years, the choice of this election equipment was the correct choice and a sound choice.

The election equipment that I have chosen is their equipment that provides a paper trail, as required by the State of Illinois, for all votes cast, whether it be cast manually through the paper ballot or using the touch-screen device, which produces a paper ballot in human-readable form at the end of the process, for which the person then has the opportunity to review that, and then they will, themselves, place that ballot into the ballot box for tabulation.

Some of the other logistics that I have to also worry about include staffing of election judges. It is very difficult to always staff my election judges adequately, but we do the best we can. Christian County, not being a large jurisdiction, has 30 precincts, and of those 30 precincts, we have 23 physical polling locations so five judges per precinct. And it sometimes is rather difficult, but we do our best to try to make sure that we have as much staffing as we can at those locations.

The election equipment, as far as custody, it stays in that locked room. It's only accessed by myself or my staff whenever we need to do any upgrades as far as programming, which is involving, of course, our election vendor, because I do have that service as well. And then we release that equipment to the election judges prior to the election so that they can take it out, get it to the precincts, and then they will bring it back at the end of the election cycle.

The cybersecurity-related responsibilities, as I described before, have become increasingly noticeable. I am a member of the MS–ISAC, the EI–ISAC, and the HSIN. I receive notices on a daily basis, multiple times a day, through emails from all of these organizations notifying me of vulnerabilities primarily to software packages but occasionally to other situations that would just allow for us to be on a heightened awareness of other attacks possibly directed to our firewall.

The situation as far as funding, of course, as a local election authority, we do receive funding through the HAVA grants, which is funneled from the Federal money through the State down to us. And I can talk about that in more detail later if you would like.

And that is all I have on my statement today. Thank you for your invitation.

[The statement of Mr. Gianasi follows:]

Michael C. Gianasi Written Testimony
Committee on House Administration
"2020 Election Security--Perspectives from Voting System Vendors and Experts"
January 9, 2020

As a newer County Clerk and Recorder in Illinois, I have been quickly introduced to the constantly evolving world of elections. As the local election authority, it is my responsibility to maintain the highest standards when conducting all facets of the election process. As members of this Committee, all of you are aware of the responsibilities as a candidate in an election, but may not be aware of all of the responsibilities of the election authority challenged with successfully completing the election process. Maintaining adequate election judge staffing levels, verifying all equipment is transported and set up at the correct precinct locations, and promptly and correctly having those election judges close the election and return the machines and results to the election authority office for tabulation are some of the tasks during the time leading up to, and including, election day.

As a small county in central Illinois (population approx. 34,000), maintaining election security has been challenging over the years. Physical security of the equipment is maintained within the courthouse where the County Clerk's office is located and the equipment is only outside the control of the storage area when the election judges transport the machines to the precincts and back at the end of election night.

Since 2016 there has been a constantly increasing pressure to advance all aspects of election security, with cyber security leading the way. Events occurring in the last several years have shown that any network has potential vulnerabilities from external and well as internal attack. The Illinois State Board of Elections, in conjunction with other organizations, has promoted the membership in the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the Homeland Security Information Network (HSIN). Multiple times each day I receive emails regarding new vulnerabilities found in hardware and software; new potential attack vectors for servers exposed to the internet, and updates concerning possible threatening activities monitored by state and federal government organizations.

Another program provided by the Illinois State Board of Elections is the Cyber Navigator program that provides guidance in the form of a person trained to assist local election authorities in determining the best uses of available resources to protect the election infrastructure and voter registration data. My office is in the final stages of completing a connection into the Illinois Century Network. The ICN will provide secure network access from my local voter registration database to the ISBE database with traffic monitoring and other security measures. I have also subscribed to a service that provides cyber security training and email phishing tests to county employees. With many successful attacks starting at the press of a button on a link in an email, it is prudent to constantly provide training to employees to recognize those threats immediately. Christian County is fortunate that Help America Vote Act (HAVA) funds are available for these expenditures.

Finally, there is the election equipment itself. The equipment used in Christian County was purchased in 2004. Reliability had been an increasing concern and the new focus on cyber security also played a pivotal role in approving the decision to lease new election equipment. My current election vendor has been providing excellent service to the county for many years, as prior clerks would attest to, and continues today. With his extensive knowledge in this area, I agreed with his recommendation for Christian County to use the Unisyn Voting Solutions, Inc., optical scan and Freedom Vote Tabulators. The security of these devices is much more substantial than the previous election hardware. This equipment will provide additional comfort to the voters that the Christian County Clerk's office is making every effort to secure the election and protect the integrity of the process and the results.

Respectfully submitted,
Michael C. Gianasi
County Clerk and Recorder
Christian County, Illinois

The CHAIRPERSON. Thank you.

And thanks to all of you for your testimony as well as your written statement.

We now have time for Members to ask a few questions. I'll first turn to the Ranking Member, Mr. Davis, for his five minutes of questions.

Mr. DAVIS of Illinois. Thank you, Madam Chairperson.

And thanks to all the witnesses. Very compelling testimony.

Mr. Gianasi, I'll start with you, since you came out here at my request. Can you tell us—I understand you recently purchased some new machines for Christian County.

Mr. GIANASI. Correct.

Mr. DAVIS of Illinois. What decisions led you to purchase those specific machines?

Mr. GIANASI. The original machines that Christian County had been using were purchased in 2004. And those machines, like I said before, the AccuVotes and such, TSX, were purchased using HAVA funds that were available at that time. Those machines, although doing well up through and including the most recent elections, have seen better days. They have outdated hardware that is no longer able to physically provide a dark print on the ballot——

Mr. DAVIS of Illinois. So they were outdated. You——

Mr. GIANASI. Yes.

Mr. DAVIS of Illinois [continuing]. Needed to get some new ones. Did you use HAVA funds to get these new machines?

Mr. GIANASI. I did not have any HAVA funds available to get these new machines. I was able to work through the county board, who had general obligation bond money available for this project——

Mr. DAVIS of Illinois. How much did that cost you?

Mr. GIANASI. I have signed what is a six-year lease on these machines. I chose not to purchase. And that six-year lease, approximately $322,000.

Mr. DAVIS of Illinois. And knowing the size of our county, that's a pretty big impact to the county budget.

Mr. GIANASI. As of Tuesday, I have 21,212 registered voters in my entire county.

Mr. DAVIS of Illinois. Okay. Great.

When you made the decision to purchase those machines, you didn't call anybody at the Federal Government and ask permission, right?

Mr. GIANASI. I did not.

Mr. DAVIS of Illinois. Okay.

You mentioned in your testimony, too, about the Illinois Cyber Navigator Program. It's a program I've talked about in this hearing room many times. I think it's a great partnership between the U.S. Department of Homeland Security and the State of Illinois and, in turn, all local election officials, like yourself.

How's this program been beneficial to your role as an election administrator in Christian County?

Mr. GIANASI. The Cyber Navigator Program is beneficial, I believe, to all election authorities and, in particular, those that do not have the resources to maintain any form of IT staff, in particular, or those that just have an inability to continue to monitor all of the problems that are coming down the line and then be able to provide solutions to those problems.

Mr. DAVIS of Illinois. So you don't have a dedicated IT staffer. You're that person, right?

Mr. GIANASI. Correct. We don't have any IT staff. The county does hire an outside IT contractor to perform all IT-related functions, including patch updates, firewall maintenance, email maintenance, et cetera.

Mr. DAVIS of Illinois. Just for your office or for the whole county, all the offices?

Mr. GIANASI. For the whole county, all offices.

Mr. DAVIS of Illinois.So the treasurer, the county clerk, the sheriff, everybody, right?

Mr. GIANASI. Correct.

Mr. DAVIS of Illinois. Now, do you find that this Cyber Navigator Program, this partnership between DHS, funded by your Federal tax dollars, is good assistance to small, rural counties like your own?

Mr. GIANASI. I do, because, again, with the changes that are happening, the Cyber Navigator who now is partnering with the county has given us the ability to promote different aspects of cybersecurity-related awareness. He's also currently directly assisting with the installation of new hardware which will provide secure access between our voter registration database server and the Illinois State Board of Elections' database server through what's called the Illinois Century Network.

Mr. DAVIS of Illinois. Excellent. Thank you for your testimony today. Thanks for being here, Mike. Great to see you.

Mr. Palmer, while I have some time left, one major element of the election infrastructure that I believe remains unaddressed are electronic pollbooks. It's my understanding that they're not currently regulated by HAVA, the Help America Vote Act, in any way. Are there security risks associated with electronic pollbooks?

Mr. PALMER. Yes, there is. And you're right, it's not regulated currently under HAVA, although there are some instances where there may be some interaction with the voting system. I think the EAC is looking at electronic pollbooks as perhaps there's a way the EAC could do a review and, sort of, approval process for electronic pollbooks.

There's a growing use of electronic pollbooks across the country. It's not universal, but more and more counties are using them because of the ease and the ability, the accuracy of electronic pollbooks. But there are some downsides to that, and so the EAC feels that we have an opportunity here.

Mr. DAVIS of Illinois. While I have a few seconds left, can you give us one suggestion or two suggestions of what you think we could do to update HAVA?

And, also, if I could ask the EAC to give us an opportunity to address some of the concerns you may have with HAVA in case this Committee and this institution wants to readdress what was passed years ago.

Mr. PALMER. Well, I think that there's an opportunity for the EAC at the Federal Government level to sort of do a review and certification program for other election systems beyond voting systems.

But the EAC and the commissioners, we would love to talk with the Committee as a whole and talk about ways that we believe, at the EAC, things that could be improved from a fundamental level.

Mr. DAVIS of Illinois. Right. Thank you.

The CHAIRPERSON. The gentleman's time has expired.

I turn to Mrs. Davis, the gentlelady from California for five minutes.

Mrs. DAVIS of California. Thank you.

Thank you very much to all of you for being here and for your experience in dealing with all of these issues.

Dr. Spearman, I wanted to just ask you, we've talked about the access issue, and you brought to the election personnel the concerns that you were having, and it sounds like they responded to you. But I'm wondering, with all of these issues, what you feel sometimes gets lost, sort of, on the radar screen in terms of what the needs of people, of voters really are in their communities that doesn't get addressed very well.

Rev. SPEARMAN. Well, as I stated—and thank you for your question, Congresswoman Davis. As I stated, I have—I guess I would respond to that by saying on the county board of Guilford County I am a rarity. I'm the only African American and I'm the only activist. I come with the concerns of the people, the concerns of the voter.

And oftentimes it seems as if the voter has been last on the totem pole. And that's something that I have been advocating for since I've been on the board, to put the people on the radar. Because the elections, as far as I'm concerned, are the people's. And the more the people, the more humans are involved in the process, I think the better off we are going to be.

As far as I am concerned right now, our democracy is an aberrant democracy. And in order to make that democracy and save our democracy, I think the people need to rise up and be counted.

Mrs. DAVIS of California. Is there a specific change that you think could or should be made in terms of easier access or, again, more voting days? I don't know, vote by mail, if that's an issue in your area?

Rev. SPEARMAN. Well, I mean, we've been fighting for that in North Carolina since 2013, since after Shelby versus Holder, and we're going to continue to fight. We just recently won another lawsuit with regard to winning a preliminary injunction for voter photo ID, which has already been a lawsuit that we won previously but it seems that the General Assembly continues to come back, disguise it in different ways, and tries to get it through again.

So, as it relates to access, one of the things that I believe would be helpful, especially to persons like myself, county board members, is more education, more training for the county board members, and just let the county board members know what it is that they are being elected to do.

Mrs. DAVIS of California. Thank you.

Dr. Blaze, I think it was also mentioned what should be done at this time to try and help with these processes. And yet we know that, in many cases, that's not going to happen before this next election in 2020. So what is it that you think we really need to be focused on very particularly in terms of hacking of any elections, intervention? What is it that you're most worried about?

Mr. BLAZE. Sure. Well, I think, you know, the things that I'm most worried about are a repeat of some of the types of attacks that we saw in 2016 against larger election infrastructure, not just voting machines themselves but the back-end systems that manage voter registration records and so on.

We've been very fortunate that even in 2016 the attacks against our systems had a relatively light touch. A determined adversary who wanted to disrupt our elections would have a frighteningly easy task if they wanted to do so. And I worry that the over 5,000 election jurisdictions who maintain these systems throughout the country are not uniformly ready to respond to a sophisticated adversary like that. So, to the extent we can support them, that is an urgent priority.

Mrs. DAVIS of California. And you mentioned that many counties don't audit. And is that because they feel that they don't have the resources to do that, they don't have additional funding? Or is it just an attitude as well?

Mr. BLAZE. Well, no, I think, you know, everybody is trying to do their best, but risk-limiting audits have not yet penetrated throughout most of the country. There are only a handful of States right now that do them. More States are starting to explore them. To the extent that we can encourage wider adoption of these, that will improve things significantly.

Mrs. DAVIS of California. Yes.

Thank you. My time is up.

The CHAIRPERSON. Thank you.

I just have a few follow up questions.

First, I want to thank all of the witnesses, but also, Dr. Gilbert, the National Academies' report was enormously helpful to us, and I want to thank you for that. It really is the guts of what we ended up putting in our SAFE Act that's now pending in the Senate. Tremendous appreciation for you and the other scientists who worked on it.

I want to talk about the ballot-marking devices. I don't love these systems. On the other hand, we need to have a capacity to allow the disability community to exercise their franchise freely, and that's an important element of providing for that.

I am concerned about the QR codes and barcodes that cannot be read by the voter. And so, really, if you're checking the paper, it really doesn't prove anything in terms of whether or not the barcode reflects what is on the piece of paper.

It's not possible that all of that will be changed between now and election day in November. What are your suggestions, as computer scientists, Dr. Blaze and Dr. Gilbert, for what could be done in the interim about that problem?

Mr. BLAZE. So—should I?

Mr. GILBERT. Yes.

Mr. BLAZE. Okay.

Ballot-marking devices were originally conceived purely as an assistive technology for voters who couldn't mark their own ballots for various reasons and were never originally——

The CHAIRPERSON. Correct.

Mr. BLAZE [continuing]. Conceived as the primary method for people for voting. It took us a bit by surprise that systems that use ballot-marking devices as the primary method of voting were being deployed and purchased by people across the——

The CHAIRPERSON. Correct. If I——

Mr. BLAZE [continuing]. Country, but there's been an——

The CHAIRPERSON. Right.

Mr. BLAZE [continuing]. Explosion of research over the last year in whether voters can reliably verify them.

What we found, most recently studied by Alex Halderman's group in Michigan, is that voters don't appear to be able to reliably confirm that their marks match what their intent was. And that's a significant—raises significant concerns——

The CHAIRPERSON. I understand that. And it's, like, 7 percent of the people, actually, according to that report.

Mr. BLAZE. That's right.

The CHAIRPERSON. But what do we do about that?

Ultimately, I think we ought to have paper ballots and these marking devices ought to be available to those who need them because of disability purposes.

Mr. BLAZE. Right.

The CHAIRPERSON. Between now and when that is achieved, what do we do?

Mr. BLAZE. The best thing we can do is voter education. The Michigan paper has some concrete suggestions on interventions that aren't perfect but they can at least increase the ability for voters to check. And, you know, it's simply a matter of the instructions given to voters, whether they're given a personal reminder to check their ballot selections. And those appear to make, you know, a significant—not sufficient, but significant difference in how well they're verified.

The CHAIRPERSON. Dr. Gilbert, do you have anything to add?

Mr. GILBERT. Yes, I have a lot to add.

So, to start, these studies—I want to make the record clear. The studies are saying that people did not verify their ballot; they didn't say they could not verify their ballot.

So I would recommend, going to the Michigan study—notice that the Michigan study said, "Remind the voter to review their ballot."

The CHAIRPERSON. It goes up to, like, 70 percent if you remind them.

Mr. GILBERT. Yes. Well, try this: "Would you please verify that your ballot selections were not changed?" Rather than, "Review your ballot." Let's try that.

The ballot-marking device—there were 16 million voters who voted with a disability in 2016. What was the margin of victory? Less than 3 million votes?

The CHAIRPERSON. Yes.

Mr. GILBERT. So if we were to design these machines so they are only used by people with disabilities, an adversary finds that as a happy day, because all you have to do is target a specific group.

Universal design, meaning more people using those machines, gives you greater security. The likelihood of catching errors increases as a result of that.

I will be honest. The universal design when HAVA was created, it was designed that each precinct would have at least one accessible voting machine.

The CHAIRPERSON. Correct.

Mr. GILBERT. I said that wasn't possible because you're going to have a separate-but-equal connotation. And they said, you can't have one machine that everyone uses. So we built it. Later this year, we'll have an announcement about a transparent voting machine, a new innovation, that will address these issues.

So, in the Academies' report, we recommended that we have a national center to do research around these things. That is a necessity. This is an arms race. It's not just going to happen and end.

To suggest that we should go back to hand-marked paper ballots is the same as saying, we had an accident on the highway and people unfortunately died, so we should return to horses and carriages.

The CHAIRPERSON. My time has expired.

But I do want to just mention, Ms. Howard, you have decertified machines that didn't meet standards. We know that we're not going to get to where we need to be between now and November. Do you have any suggestions on what interim steps we could take to make the systems safer?

Ms. HOWARD. Well, yes. Thank you for the question.

So two basic things, right? Voter education about how to use the machines is very important. And, additionally, there must be post-election audits which rely on the human-readable portion of the ballots even if the ballots do include barcodes.

The CHAIRPERSON. Thank you.

My time has expired. All time has expired.

I would like to thank each of you for your testimony. Note that, because we didn't get a chance ask all our questions, we may follow up with written questions for you, and, in that case, we'd ask that you answer promptly.

[The information follows:]

HEARING
COMMITTEE ON HOUSE ADMINISTRATION
"2020 ELECTION SECURITY-PERSPECTIVES FROM VOTING SYSTEM VENDORS
AND EXPERTS"
JANUARY 9, 2019
MAJORITY QUESTIONS FOR THE RECORD
FOR
MR. TOM BURT
PRESIDENT AND CEO, ELECTION SYSTEMS & SOFTWARE

Federal Reporting Requirements

1. During the testimony of Mr. Burt, he testified he would support federal reporting requirements specified below. Please provide the following information to the Committee:

   a. ES&S's cybersecurity practices, including incident response procedures.

ES&S has a formal written information security policy. This comprehensive document, which is reviewed annually and was last updated in June 2019, covers all aspects of ES&S' security policy, including, but not limited to, access control, asset management, physical and personnel security, data management, business continuity, and network and removable media controls.

ES&S employs multiple measures to monitor ongoing security threat changes and respond to evolving threats. ES&S has installed Albert sensors in the voter registration environments it hosts for customers. ES&S allows the Department of Homeland Security (DHS) National Cybersecurity Assessments and Technical Services (NCATS) team access to scan its public-facing internet presence weekly, looking for vulnerabilities. ES&S works with multiple federal, state and local entities to be informed of and manage security risks to its hardware, software and services. ES&S subscribes to multiple cyber threat notification feeds that allow it to assess and react to any security threat posed to its systems or its customers. These cyber threat feeds originate from the U.S. Intelligence community, U.S. law enforcement, DHS, the Multi-State Information Sharing and Analysis Center (MS-ISAC), the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), and the National Cybersecurity Communications and Information Center (NCCIC). ES&S uses the same common vulnerabilities and exposures (CVEs) system that the federal government uses to rank cyber risk and assign corresponding resources to mitigate those risks where applicable to ES&S products. ES&S is a supporting member of the EI-ISAC, a member of the Information Technology Information Sharing and Analysis Center (IT-ISAC) Election Industry Special Interest Group (EI-SIG), and ES&S' Vice President of Systems Security is also the past Chair of the Elections Infrastructure Subsector Coordinating Council (EI-SCC), and currently serves on the Executive Committee of the same.

ES&S has a comprehensive security plan and training program that all employees, contractors, temps and interns (ECTi) are required to follow as a condition of employment or engagement. The company requires all ECTis to use multi-factor authentication as part of its multilayered corporate security program to ensure if a user's access credentials are lost or stolen that they cannot be used to access the corporate network. Security indoctrination and awareness training initiate during the first week of onboarding when each new ECTi meets with ES&S' VP of Systems Security, where he provides a briefing on the ES&S security awareness and training plan. At the time of onboarding, each ECTi is required to complete a comprehensive computer-based security awareness training program. This training program, procured from world-class security training firms, is updated frequently. The program covers a wide range of cyber and physical security threats, mitigating controls, realistic scenarios and content module tests that the trainee must pass successfully as a prerequisite to obtaining continued access to company network resources. This training program emphasizes good cyber hygiene to be used at home and at work to build respect for and awareness of cyber threats to ES&S' business. The completion date of this initial training becomes the anniversary date and basis for the company's training department to track the completion of the training on an annual basis thereafter.

ES&S also uses enterprise phishing training tools. All ECTis are automatically enrolled and phished by the automated program on a regular recurring basis. Users who fail the phishing exercise are provided immediate feedback on what they did wrong. Users who fail the phishing exercise more than once receive additional remedial training designed to increase awareness of the phishing threat and the consequences of continued risky behavior. Repeat offenders can be deemed in non-compliance with ES&S job requirements, and appropriate actions will be taken.

Additionally, the VP of Systems Security, supported by the corporate Security Awareness Team, and Human Resources and Marketing Departments, communicates cybersecurity awareness of issues and best practices through regular (monthly and bi-weekly) communication campaigns using email, workplace posters and bulletins. ES&S also conducts quarterly informational "security lunch-and-learns" where ECTis receive timely, interactive information on security.

ES&S follows the 2018 DHS publication titled: *Incident Handling Overview for Election Officials* that instructs election entities on how to inform DHS about cyber-related incidents. ES&S has a mature, tested incident response policy and process whereby potential cyber incidents are triaged by ES&S' internal team of subject matter experts and whereby circumstances indicate the reporting of the incident to government officials. ES&S follows DHS guidelines for alerting the NCCIC, MS-ISAC and EI-ISAC.

ES&S uses its internal corporate information security staff to receive, evaluate and act upon, as necessary, vulnerability reports received from software manufacturers, cybersecurity researchers and other third parties.

ES&S employs an eight-step incident response plan including: 1.) initial triage; 2.) communications with customers; 3.) engagement with vendor partners and law enforcement; 4.) full incident triage; 5.) incident containment; 6.) incident eradication; 7.) system recovery; and 8.) restoration of services.

b. Any cyberattacks ES&S has experienced. This should include any phishing attempts ES&S has detected.

There are no known successful cyberattacks on any ES&S election technology deployed in the field and no evidence of any voting ever having been affected.

Just like any private business or governmental entity, ES&S experiences continuous scans of its external networks. These scans are detected and repelled by ES&S' layered security defenses. ES&S has also experienced numerous phishing attempts of its employees, all of which have been unsuccessful to date because of ES&S' comprehensive employee cybersecurity awareness and internal phishing training campaigns.

c. Personnel policies and procedures, including whether background checks and other procedures are in place to safeguard against inside attacks and how ES&S assesses current employees on an ongoing basis for security risks. Please specify the policies and procedures.

ES&S requires completion of a background check for any candidate (including contractors) applying for employment with, or engagement by, ES&S. The background check must be successfully completed before commencement of employment or engagement.

All background checks include, but are not limited to, the following:

i. County Criminal background check
ii. Federal Criminal background check
iii. Global Criminal background check
iv. Nationwide Criminal background check
v. Sex Offender background check registries
vi. Statewide Criminal background check
vii. Motor Vehicle records, including:
    1. Violations/convictions/failures to appear
    2. Suspensions/revocations
    3. License and permit information
    4. Miscellaneous State data
    5. Fingerprinting where required

d. Details of corporate ownership and foreign investment. Please submit a list of all individuals and entities with a five percent or more ownership or control interest in ES&S, including private equity investors, and indicate the percentage of ownership or controlling interest. Please also provide a list of all investment by foreign entities and individuals in ES&S.

Government Systems, Software & Services, Inc., a Delaware corporation – 100%
Foreign Investment – None

e. Details on ES&S's supply chain, including where parts, software patches, and installations come from; how are they transported; and how they are kept secure.

ES&S, like many other companies, necessarily participates in a global supply chain. Parts are only sourced from authorized distributors. Some suppliers are based in the U.S., while others originate in other countries, including countries in Asia. Responses to questions in section 3 (below) provide more specifics on countries of origin.

All software for ES&S tabulation products is written and housed exclusively within the U.S.

Each part, regardless of origin, undergoes a thorough incoming inspection by ES&S contract manufacturers prior to the assembly process. Once units are assembled, ES&S uses a domestic third-party expert to perform firmware verification on a sample of units in each container to confirm no malicious or unwarranted software is present.

Finished goods are stored in secure warehouses where they undergo final configuration and quality control. Badge readers and video cameras secure ES&S' warehouses and production facility. All equipment is shipped to customers in secured trucks and installed at customer sites by trained technicians under the observation of election officials. During this installation, the trained technicians will complete a final check of the firmware loaded on each unit. Customers also perform an independent final acceptance check verification.

Other Reporting Requirements

2. In addition to reporting the information above discussed during the hearing, please provide the following information to the Committee. This is all information that ES&S is required to provide to at least one of the states in which its machines are certified:

a. Management and staff organization; number of full-time employees by category; and number of part-time employees by category.

Senior leadership	24	Individual employees	387
Department directors	20	Part-time employees	2
Managers	45		

b. Financial history of the business, including a financial statement for the past three fiscal years.

ES&S has been serving the needs of election administrators for more than 40 years. Thanks to superior products, customer service and stable ownership, ES&S' customers have rewarded its efforts, and the company has steadily grown over the past 33 years. ES&S' balance sheet is one of the strongest in the industry, and this is reflected in the company's level of service commitment to its customers. As a privately held company, ES&S does not publicly release its financial statements.

c. History and description of the business, including year established; products and services offered; states with machines ES&S's manufactures or services; branch offices and subsidiary and/or parent companies.

In 1980, American Information Systems (AIS) entered the election industry to provide innovative solutions to vote tabulation. At the time, AIS was known as the leader for central scanners and tabulators. Five years later, Business Records Corporation (BRC) acquired Computer Election Systems in Berkeley, California, to enter the industry.

AIS and BRC joined forces to form Election Systems & Software and dedicated itself to incorporate the highest quality scanning solutions into precinct and central scan tabulation. Since that partnership began, the philosophy has remained consistent – provide better elections every day. ES&S is a subsidiary of Government Systems, Software & Services, Inc. (GS3). GS3 also is a parent to ESSVR, which is ES&S' voter registration solution.

Fast-forward to today, ES&S is still dedicated to that mission and provides products and services to jurisdictions in 41 states and Washington D.C. (not present in AK, CT, GA, HI, NH, NM, OK, VT, LA). Solutions have expanded over the years, but still include precinct and central scanners and tabulators. In addition, ES&S provides counties with electronic pollbooks, ballot marking devices, election management software, ballot printing and professional services, including implementation, on-site support and training.

ES&S' headquarters are in Omaha, Nebraska. To provide states, counties and local jurisdictions with timely service, close to half of the company's roughly 500 associates work in the territory they support. ES&S has offices in Richardson, Texas; Birmingham, Alabama; Jackson, Mississippi; and Rockford, Illinois.

d. Audited report of the business' fiscal year 2019.

As a privately held company and a matter of practice, ES&S does not publicly disclose financial information.

Supply Chains

3. During the January 9, 2020, hearing, Mr. Burt could not provide the Committee with the precise percentage of components from China on the spot. For all the questions below, please also provide specifics on the relevant components by describing them; whether they are inert or programmed or programmable; and the machines for which those components are used.

   a. Please provide the percentage of the components in ES&S's supply chain that come from China.

   b. Please also provide the percentage of components in ES&S's supply chain that come from foreign countries other than China. Please provide the country and percentages by country.

   c. Please provide the percentage of components come from China-based companies.

   d. Please provide the percentage of suppliers in ES&S's supply chain that have locations in either China or Russia.

Responses for a, b, c & d above

ES&S has put significant actions and preventative steps in place to ensure the integrity of every aspect and component of its supply chain. These multiple layers of protection, developed in consultation with leading experts in supply chain security, include using only authorized suppliers for parts acquisition, incoming parts inspections, quality control checks, firmware verification audits, QC configuration and equipment testing at customer sites. All steps are overlaid by the physical security of ES&S' facilities and its product offerings.

From the standpoint of security, not all parts are equal. Many parts are inert and cannot be compromised, such as a plastic shield for voting privacy. ES&S' top, most robust security measures are in place for any part considered to be a Programmable Logic Device (PLD). PLDs contain software, firmware or low-level settings, and they control how the equipment operates.

Answers provided below pertain to ES&S' leading precinct-based tabulation and ballot marking devices and do not include all of the accessories (e.g., cases, booths, marking pens, paper rolls). ES&S sells hundreds of products, many of which do not include any electronic components.

The part counts in the charts below reflect the parts that are ordered by ES&S' contract manufacturers to produce a given finished good. Each of these parts may have sub-components that may come from other countries.

ExpressVote Bill of Material: Country of Origin

Country	Part Count	%	PLD Part Count	%
China	158	37.9%	0	0%
Taiwan	149	34.4%	1	12.5%
Japan	41	9.5%	0	0%
Malaysia	29	6.7%	1	12.5%
Mexico	13	3.0%	1	12.5%
Singapore	10	2.3%	0	0%
Philippines	8	1.8%	1	12.5%
Thailand	8	1.8%	3	37.5%
Multiple	7	1.6%	0	0%
USA	6	1.4%	1	12.5%
Israel	2	0.5%	0	0%
Germany	1	0.2%	0	0%
India	1	0.2%	0	0%
Total	**433**	**100%**	**8**	**100%**

DS200 Bill of Material: Country of Origin

Country	Part Count	%	PLD Part Count	%
China	112	38.1%	1	11.1%
Taiwan	76	25.9%	2	22.2%
Japan	24	8.2%	1	11.1%
Malaysia	18	6.1%	0	0%
Mexico	14	4.8%	0	0%
USA	14	4.8%	2	22.2%
Thailand	11	3.7%	1	11.1%
Multiple	10	3.4%	0	0%
Philippines	7	2.4%	2	22.2%
Singapore	4	1.4%	0	0%
Vietnam	2	0.7%	0	0%
India	1	0.3%	0	0%
Indonesia	1	0.3%	0	0%
Total	**294**	**100%**	**9**	**100%**

4. In addition to concerns about the components in ES&S's supply chain, the Committee requests more information on ES&S's software development.

   a. Where is ES&S's firmware and software developed? If it is developed in multiple locations, please specify those locations.

   All ES&S firmware and software is developed in Omaha, Nebraska, and Rockford, Illinois.

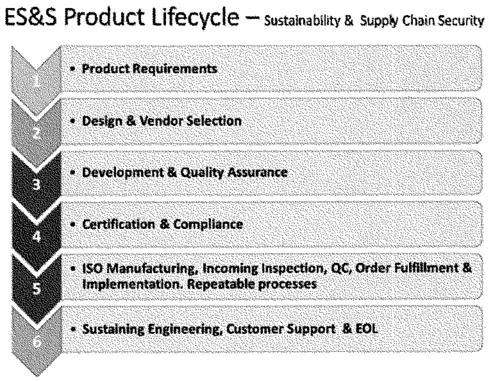
   b. Where is it installed?

   All ES&S firmware and software is installed in Omaha, Nebraska. Software upgrades to firmware and software are performed in Omaha or at the customer site.

   c. How does ES&S protect it from remote access and tampering from outsiders? Please provide specifics.

   Software development and installation is performed in isolated network environments that are logically separated by subnets and virtual LANs and are behind firewalls that are updated, managed and monitored. There is no remote access to software and firmware environments.

5. For components that are manufactured in other countries, like China and Russia, is it possible for you to find different manufacturers that are in the United States or in countries that have not been accused of committing cyberattacks against the United States? If not, why not? For example, is the component protected by a patent?



ES&S Product Lifecycle – Sustainability & Supply Chain Security

1 • Product Requirements

2 • Design & Vendor Selection

3 • Development & Quality Assurance

4 • Certification & Compliance

5 • ISO Manufacturing, Incoming Inspection, QC, Order Fulfillment & Implementation. Repeatable processes

6 • Sustaining Engineering, Customer Support & EOL

ES&S controls more aspects of the company's election equipment than other providers in the elections industry because the company uses a purpose-built product strategy. The chart above shows how ES&S manages its product life cycle from initial design concept to end-of-life, including every step in-between. No parts are procured from Russia, and ES&S minimizes procurement from China wherever possible or practical. ES&S pays particularly close attention to and has robust security protocols in place for sensitive items like PLDs. ES&S' Engineering Team continually reviews the ability to source components elsewhere. If the ability exists to source needed components outside of China, ES&S instructs its buyers and contract manufacturers to follow protocol.

In some instances, there is no ability to procure from alternative component suppliers. Some components are sole-sourced, protected by a patent and/or intricate to the design of the circuit or sub-assembly. ES&S' experts evaluate the risk and impact of using that specific item. The company also assesses safeguards to limit risk when using sensitive components in its product offerings. Every aspect of ES&S' system is under engineering revision control, regardless of where the individual components are produced.

6. In ES&S's response to the Committee's September 19, 2019 letter asking questions about how ES&S protected the security of its supply chain, ES&S provided some best practices which it follows. How specifically does ES&S know that its best practices are working – if they are – and that its supply chain is secure? What checks does ES&S have in place?

ES&S' purpose-built tabulation machines include commercially available components configured and manufactured to a custom design for a specific use. ES&S voting systems are produced in ISO-9001 manufacturing facilities. The entire voting system is managed by a secure engineering change order control process. This testing includes all components and suppliers. Changes to the voting system follow a formal closed-loop process and must be internally and externally reviewed, verified, tested and approved before they can be incorporated. Every unit is individually serialized for complete traceability.

ES&S conducts thorough security reviews of its supply chain, including supply chain risk assessments using National Institute of Technology (NIST) Cybersecurity Framework (CSF) tools, combined with on-site visits of ES&S' suppliers, to ensure that every component is trusted, tested and free of defects. All tabulation software is produced and compiled exclusively in the United States. All components of the hardware go through a formal incoming inspection and testing process. Final hardware configuration control and quality assurance are performed at the company's headquarters in Omaha, Nebraska.

As a standard practice, each hardware and software release undergo thousands of hours of performance testing and millions of test ballots, along with extensive security testing, after which ES&S provides a complete set of software components to the voting systems testing labs (VSTL) for review. ES&S is participating in discussions with DHS's National Risk Management Center (NRMC), NIST and the Center for Internet Security (CIS) regarding the development of guidelines and best practices for ensuring that the company stays ahead of and mitigates new or emerging risks associated with supply chain components.

ES&S carefully monitors all software that is included in its solutions to ensure that these solutions continue to be secure. If any gaps are highlighted in these software products, ES&S works with the software provider to ensure that the gap is mitigated either through software updates or segmentation of the software.

Part of each ES&S software release includes a review of all software components included in the release. This review includes an analysis of the security features and any highlighted vulnerabilities. Additionally, ES&S' security team carefully monitors all highlighted vulnerabilities to determine if any action is required to address the vulnerability.

All ES&S Election Management Systems either stand alone or are part of a closed network. However, to protect against malicious software, ES&S recommends that its customers maintain systems in the same hardened configuration in which they were installed, which includes the following safety measures:

- Required installation of anti-virus software. Installed anti-virus must match the type and version tested and certified to Voluntary Voting System Guidelines (VVSG) standards for use with the voting system.
- Require the firewall to be enabled on all networked systems.
- Disable support for Internet connections
- Disable the routing, DNS and gateway services.
- Configure various TCP/IP parameters in the Windows registry to protect against network-level denial of service attacks, including SYN flood attacks, ICMP attacks and SNMP attacks.

7. Interos wrote on page five of its report *Election Technology & the Global Supply Chain* that it notified the manufacturer of the machine that was the subject of the report.[1] The report stated that "Interos recognizes the extreme sensitivity of election security matters and has contacted the affected company involved." Has ES&S been notified by Interos that it is the vendor that manufactured the machine discussed in the report?

No.

ES&S VP of Systems Security Chris Wlaschin was contacted by Interos in his role as Chair of the SCC, but at no time did Interos indicate that ES&S was the subject of the report.

[1] *Election Technology & the Global Supply Chain*, Interos, (Dec. 16, 2019), page 5, https://cdn2.hubspot.net/hubfs/5812029/Interos%20-%20Election%20Security%20Paper.pdf.

ES&S welcomes the guidance of cyber and supply chain security experts and has taken significant steps to implement policies as a result. The practice of assessing risk based solely, or even primarily, on the geography of a supplier's corporate locations is a practice that has been widely discredited. Supply chain risks and threats exist regardless of where a company is located or where its products are manufactured or assembled. As NRMC Director Bob Kolasky noted in recent congressional testimony on this subject, "sources of material influence" must be evident. The only conclusive statement in the release is that "none of [Interos'] findings indicate that the studied machines are compromised in any way."

8. What steps does ES&S take, if any, to ensure that subcontractors and manufacturers producing its components overseas are not subject to influence from a foreign government?

   During the vendor selection stage of its product life cycle, ES&S meets with top engineers and management to evaluate their ability and willingness to meet the company's revision control notification requirements before changes are implemented. The companies that makeup ES&S' supply chain are certified and audited by International Organization for Standardization "ISO." This requirement ensures established processes and protocols are followed.

Ballot Marking Devices

9. Studies on the use of ballot marking devices show that voters check their ballots at very low rates and alert election officials to errors at an even lower rate. Is ES&S working to design ballot marking devices or to identify other technical solutions that improve the rate of voter verification of their printed ballots to ensure that there is a reliable voter-verified paper trail from its ballot marking devices that can be audited with confidence?

   A voter is fully able to read and verify his or her selections in the printed text on a paper ballot that they marked using a machine, just as a voter can read and verify their selections on a paper ballot marked with a pen. A recent study by Dr. Michael Byrne at Rice University analyzed voter behavior and whether voters would be able to detect anomalies on paper ballots printed by a ballot-marking device. One of the ballot styles tested in the study was similar to an ES&S ExpressVote ballot. The study results showed that of those voters who chose to examine the printed ballot, a majority of voters – 76 percent – could reliably detect errors on his or her ballot if he or she simply reviews it. These results affirm that people actually *can* verify the accuracy of their selections if they will simply take the time to review their selections before casting their ballots. ES&S works with jurisdictions to review best practices on polling place management and encourages voters to review their selections on their paper ballots before casting them.

10. Some experts in election security have raised significant concerns about the risk of ballot marking devices that store information about the choice a voter made on their ballot in a non-transparent format, such as a barcode or QR code. During the testimony of Mr. Burt,

he confirmed that ES&S sells equipment that tabulates votes based on a barcode or QR code.

a. Please specify how ES&S's ballot marking devices tabulate votes.

When used as a marker, ES&S' ballot marking device – the ExpressVote – does not tabulate votes. Rather, the machine prints a physical tabulatable paper record of a voter's on-screen ballot selections. That paper can then be reviewed by the voter by visually reading the paper or reinserting the ballot card into ANY stand-alone ExpressVote unit (*This process is fully explained in the answer to 10 d.)* before the voter takes it to a precinct scanner to tabulate his or her votes.

Some versions of the ExpressVote also have the ability to be used as a marker or tabulator. In this case, election officials must have the proper software and firmware versions to code their elections to use the machine's secondary tabulation function. All tabulation takes place by scanning the printed paper ballot. In all cases, voters have the ability to view and verify their paper record before submitting for tabulation. The paper record provides election administrators the ability to audit the election using human-readable text.

There are several important facts to note about how tabulators count ballots whether a voter makes his or her selections using a machine or fills in ovals by hand. Barcodes exist on both hand-marked paper ballots and machine-marked paper ballots, and those barcodes are used in the very same manner in both scenarios to count votes. Here is how tabulation devices read paper ballots on which a voter hand-marks their selections by darkening an oval:

- On a hand-marked paper ballot, there is a master barcode along the left edge and top and bottom of the ballot.
- When a voter hand marks the oval next to candidate Jane Doe, for example, and inserts that hand-marked paper ballot into a tabulation machine, that tabulation machine is not reading the name, Jane Doe. In fact, the tabulation machine does not recognize the text, Jane Doe, at all. Rather, the tabulation machine first recognizes, through digital imaging technology, that an oval has been filled in. Then it uses the master barcode on the ballot to determine the grid coordinates of that filled-in oval.
- In this example, if the grid coordinates of the filled-in oval are "six down, four across," the tabulation machine then queries the database that resides on the master media (typically a USB stick) that has been inserted into the tabulator. In essence, the tabulation machine asks the database on the master media, "what candidate's name is associated with six down, four across?" The database, which has been pre-programmed and tested by the county/city election office, then tells the tabulation machine that "six down, four across" corresponds with Jane Doe. At that point, the tabulation machine creates a cast vote record that records a vote for the name Jane Doe.

Jurisdictions perform pre-election logic and accuracy tests and post-election audits to ensure the accuracy of the process. During both the pre-election tests and the post-election audits, jurisdictions are asking whether the actual text next to the filled-in oval on the hand-marked paper ballot corresponds exactly to the vote that was registered by the tabulation machine. This verification can only be done if the jurisdiction has access to the paper ballot and the cast vote record from the tabulation machine. As noted above, pre-election testing and post-election auditing provide a testable and auditable method to verify that ballots are programmed and counted as intended.

Tabulation of paper ballots where a voter makes his or her selections by using a machine behaves in the exact same way. Here's how:

- When the voter chooses Jane Doe on the touch screen, the marking device prints out a paper record that shows the text Jane Doe along with a barcode that contains the ballot coordinates of "six down, four across." When that paper record is inserted into the tabulator, it performs the same routine as it does with the hand-marked paper ballot. It reads the barcode, which reveals the grid coordinates of "six down, four across." Then it queries the database on the tabulation machine (which is the same tabulation machine that counts the hand-marked paper ballot) asking which candidate name is associated with those grid coordinates. The database then reveals to the tabulation machine that "six down, four across" corresponds to Jane Doe. At that point, the tabulation machine creates a cast vote record for Jane Doe.

Just as is the case with hand-marked paper ballots, the tabulation machine is only looking for the grid coordinates, and the cast vote records from both examples are identical.

Even tabulation systems that use Optical Character Recognition (OCR) incorporate the use of a barcode to count the vote. Here's why: It is possible that there could be two separate and distinct candidates, both named Jane Doe, who are running for different offices on the same ballot. The system cannot use OCR to read "Jane Doe" and record a vote reliably because it would have to know for what race the vote for "Jane Doe" should be counted. Thus, the barcode is used to tell the tabulation machine for what race Jane Doe should receive a vote.

In sum, all tabulation machines that count paper ballots use a barcode to determine how to properly and accurately count the vote. The security of each method of voting is confirmed by election officials during pre-election tests and in post-election audits.

b. What steps does ES&S take to ensure that voters can be confident that their choices will be counted accurately?

ES&S takes immense pride in the quality of its products and services, including the security and reliability of its voting machines. ES&S' systems are independently tested and federally and state approved through thousands of hours of testing with millions of ballots. Election officials have used ES&S products in tens of thousands of successful elections. Every system ES&S supports is auditable. Jurisdictions validate the accuracy of elections through pre-election logic and accuracy testing, as well as post-election audits, to ensure that every ballot is counted as cast.

c. Has ES&S re-evaluated selling it given these concerns?

There is zero data to support the unfounded claims regarding the use of barcodes in voting system technology. As noted in response to question 10 a., barcodes are used to tabulate all ballots – including hand-marked optical scan ballots. Many security experts agree that barcodes are a successful, reliable way to tabulate and audit votes, including Juan Gilbert, Ph.D., who also testified before the committee. In his written testimony, Dr. Gilbert writes,

> "In my opinion, the gold standard for securing elections should be the audit. If necessary, a full manual recount should be possible. With this in mind, the BMD has an advantage over hand-marked paper ballots. Hand-marked paper ballots will suffer from ambiguous marks that are left to the auditors to interpret. This doesn't happen with the BMD. Some may say that the number of ballots that have this issue are small, but we have seen margins of victory very small, even down to one vote. Most importantly, every vote should count, and every ballot should be auditable."

d. Are the barcodes or QR codes used by ES&S's ballot marking device readable by any off the shelf barcode or QR code scanner?

Voters can verify their selections by visually reading the paper or reinserting the physical paper record into ANY stand-alone ExpressVote unit. The ExpressVote unit will then read back in audio form or present the choices on the screen so that the voter can validate his or her selections. As a barcode represents a numeric code, an off-the-shelf barcode scanner would be able to read the numeric code of the grid coordinates for the voter's selected candidate, in the same way that a darkened oval represents the grid coordinates for the voter's chosen candidate.

Guidance on Identifying and Mitigating Security Risks

11. As we discussed during the hearing, the Consumer Product Safety Commission advises manufacturers of consumer products to "identify all reasonably foreseeable hazards associated with" their products and include safety warnings and steps to reduce risk in the user guides. There are similar requirements for motor vehicles and warnings in owner's manuals. During the hearing, Mr. Burt testified he would support a requirement for voting system vendors to provide guidance to customers identifying security risks associated with use of ES&S's equipment and recommendations to mitigate those risks.

a. Does ES&S currently include such guidance for election officials buying its products?

Yes, ES&S conducts security seminars, provides technical bulletins and other best practice documentation, provides for an engineering change order process to upgrade needed components, and continuously provides its customers with software upgrades designed to mitigate any new or emerging risks. As noted in the company's testimony, ES&S supports additional state or federal security measures that would apply to all voting system providers in the United States.

b. If yes, please detail what is included.

See above.

c. If no, isn't it reasonably foreseeable that an election official might need that guidance or warning, particularly in the current threat environment? Why does ES&S choose not to provide such guidance? Does ES&S have any plans to do so in the future?

See above.

d. Does ES&S provide any instructions concerning audits? Does ES&S recommend risk-limiting audits?

ES&S fully supports audits, and its equipment provides the ability for auditing, either with paper ballots or digital images. ES&S supports the policy decisions of individual states regarding how they decide to perform audits or recounts, including risk-limiting audits.

e. Given the security concerns around logic and accuracy auto-testing, and the failures that happened in Northampton County, PA in 2019,[2] does ES&S recommend manual logic and accuracy testing for every ballot style? How many of ES&S's machines have an auto testing feature?

State and local jurisdictions determine logic and accuracy (L&A) requirements and procedures. Per customer requirements, ES&S provides options to automate portions of the L&A process and recommends that manual testing always be completed, including the testing of every ballot style for each election.

The ES&S ExpressVote, ExpressVote XL and ExpressTouch, used for curbside and Americans with Disabilities Act (ADA) voting, each have automated L&A features. ES&S voting systems provide the ability to generate automated test ballots, which are compatible with each of its tabulators (DS200, DS450, DS850, ExpressVote, ExpressVote XL). This functionality helps users create accurate test ballots without having to create them manually. Manual test ballot creation can require the creation of tens of thousands of ballots – a manually intensive, lengthy process that is highly prone to error. Customers determine which procedures and methods are employed.

[2] Tom Shortall, *No Confidence: Northampton County election board 'extremely disappointed' in machines it selected*, The Morning Call (Dec. 19, 2019), https://www.mcall.com/news/local/mc-nws--20191220-xrkqrrokfrgzlc3lglpn5nf5fe-story.html

f. What other election day support does ES&S provide to its customers? If this varies based on the contract, please provide specifics on the different contracts ES&S has and the support provided in each and the price difference between the levels.

ES&S provides both on-site and phone help desk services for its customers on election day. These services typically consist of equipment issue resolution, software support and absentee ballot counting. The nature and extent of services can vary from customer to customer, based upon their specific needs. Some election day support services are memorialized in a contract, while many are requested on an as-needed basis. Pricing can vary based upon the nature and extent of services required.

Cybersecurity Protections

12. During the hearing, Mr. Burt confirmed that ES&S employs a chief information security officer.

a. What is that individual's title?

The individual's title is Vice President, Systems Security and Chief Information Security Officer (CISO).

b. How long have they been on staff?

This individual has been on staff for two years.

c. What authority do they have within the company?

This individual reports to the ES&S President and CEO and is authorized to drive security innovation, modernization and improvements across all product lines, corporate IT, physical security and customer relations.

d. Does that person hold any other titles or responsibilities within the company?

This individual also has responsibility for ES&S's corporate IT structure.

13. Does ES&S have technical staff with cybersecurity expertise involved in all stages of the product—the marketing, the design, the testing, the service, and support?

ES&S employs technical staff with cybersecurity expertise in all phases of product development, including design, product development, Quality Assurance (QA) testing and customer service, but not in marketing. The VP of Systems Security and CISO advises the Marketing Team on cybersecurity matters.

14. When ES&S, or someone ES&S contracts with, assists jurisdictions with programming services, how are those files delivered to the jurisdiction? What steps do you take to ensure the transfer and delivery of the programming files is secure? What steps do you take to secure the device the programming actually takes place on?

Programming files have two different delivery methods. Method one is a digital file transfer, using an encrypted Secure File Transfer (SFT) site. In this scenario, files are hash validated upon upload and download to ensure they have not been altered. Only specific users are authorized to the SFT site, using complex passwords that expire regularly. Once the files are downloaded, they are moved to a secure customer Election Management System that is hardened for programming and not connected to the internet.

Method two is the physical shipment of the programming memory devices. The election programming is performed from a secure certified system that is not connected to the internet. The programming is thoroughly tested in-house using the same certified systems and versions as the customer. At the customer's request, a set of pre-marked test ballots are also provided so that the customer can run the same set of ballots and ensure they get the same results from the testing ES&S performed prior to shipment of the programming. Shipments are only performed using delivery services with signature tracking required so that the company is aware of who accepted the package and when.

Voting System Vulnerabilities and Updates

15. The Election Assistance Commission (EAC) issued a Notice of Clarification on De Minimis Software Changes in November of 2019.

a. Has the EAC's Notice of Clarification on De Minimis Software Changes made the certification of security updates easier?

Yes. Since NOC 19-01: Software De Minimis Changes was approved for use on November 15, 2019, ES&S has successfully used the new certification procedure for five voting system enhancements, one of which addressed recent Microsoft Windows published vulnerabilities.

b. Has that Notice solved the issue with delays to the certification of security updates?

Yes. ES&S regularly reviews vulnerabilities for all its voting equipment and systems. When a vulnerability is discovered, the ES&S Vulnerability Review Team assesses the vulnerability to determine if it affects any ES&S products. When a vulnerability is determined to be critical in nature, ES&S notifies affected customers and immediately initiates the Engineering Change Order (ECO) process in accordance with the EAC Testing and Certification Program and NOC 19-01.

Internally, ES&S must first identify all voting system releases that are affected by the vulnerability and procuring the patch from Microsoft. The process for incorporating the Windows patch into the affected voting system releases requires test planning, system integration, quality assurance and pre-certification testing by the ES&S Development and Certification teams prior to the involvement of the EAC and one of the EAC accredited VSTLs. A request for certification is then submitted to the EAC and the VSTL initiating the certification process. Installation procedures and staged Windows patch files, along with ES&S internal test results, are included as part of an ECO package provided to the VSTL for use in its assessment. The installation procedures are validated by the VSTL to confirm the patches install and perform in accordance with EAC VVSG. Once the VSTL has completed its testing, the ECO, VSTL test report and VVSG compliance assessment are forwarded on to the EAC for final evaluation and approval.

In the example of the Microsoft Windows 10 security patch, the process took 16 calendar days from submission to the VSTL for evaluation and testing and for EAC final approval for use to be issued.

c. How does ES&S ensure that states receive security updates for their voting systems?

Upon receipt of EAC approval of the Software Engineering Change Order (SW ECO), ES&S State Certification Managers submit the EAC approved SW ECO, along with supporting documentation, to the applicable states for approval and authorization to proceed with the distribution and upgrade to the affected jurisdictions.

d. On average, once an update is certified, how long does it take for a state to receive that security update?

While ES&S does not have a lot of history with state approvals of software ECOs yet, the approval period will vary from state to state due to varying statutory rules and regulations in each. Generally, ES&S expects ECOs to take anywhere from two weeks to two months, depending on the state's time frames. Often it will also depend upon the election calendar in the state.

e. How is the security update transmitted to the local election officials? What are the costs associated with getting a security update or patch?

The jurisdictions are instructed to contact the VSTL directly to receive the security update and installation instructions to their systems. In the event the jurisdiction requests the services of ES&S to perform the system upgrade and verification of the systems, there may be associated costs for this service. Otherwise, there are no costs for the jurisdiction to acquire the security patch.

16. Your company regularly submits updated voting systems to the EAC for certification.

a. Once an updated system is certified, do jurisdictions have the opportunity to update their systems?

Yes. Modifications are permitted under the EAC Testing & Certification Program. A modification is any change to a previously EAC-certified voting system's hardware, software or firmware that is not a de minimis change. Any modification to a voting system will require testing, review and approval by the EAC, as well as the approval of the state voting system certification body.

b. How does this process work? For example, is a physical intervention needed?

Once a voting system has been approved for use by the state certification body, ES&S will notify the jurisdictions of the availability of the new release and offer the opportunity for them to update their current system to the newer release. Jurisdictions are made aware of the primary features and benefits of the new release, but the decisions of whether to upgrade and when to do it, rest with state and local election officials. Upgrades to ES&S firmware and software are performed manually under the guidance of state or local election officials. There is no use of wireless technology to perform upgrades.

c. Is the process different if the update is certified by the EAC as a new system versus a modification?

No. The state certification process is typically the same whether the system is a new system or a modification to an existing system.

d. For machines that run a version of Windows that has reached the end of its life, will ES&S provide updates to jurisdictions?

Yes. ES&S does provide upgrades for end-of-life components of systems. It should also be noted that unlike other business enterprises that use Windows, the ES&S Election Management System operates in a locked-down, closed and hardened environment. When the system is configured as certified, it is not exposed to the public internet. This means that the jurisdiction's system is protected from risks commonly associated with other systems that interact with the internet. Jurisdictions can continue to use these systems in a secure manner by following the recommended security best practices, even though additional Windows security updates may not be available. No ES&S voting tabulators operate on a Windows platform; therefore, they are not subjected to Windows end-of-life scenarios.

e. If so, what will the process be for those updates and will ES&S be charging jurisdictions for those updates?

In the event ES&S finds itself in a Windows end-of-life scenario where security updates are no longer available, and updates are limited to new features and other types of security improvements, the process for both federal and state certification and opportunities for jurisdictions to upgrade remain unchanged. Fees for jurisdictions receiving modifications are determined by the agreements in place with each jurisdiction.

17. In ES&S's October 18, 2019 response to the Committee on House Administration's oversight letter, ES&S told the Committee that it is required to "report certain issues (i.e. malfunctions) to the EAC following each federal election."

a. Does ES&S also disclose to its customers and to the EAC vulnerabilities discovered from other sources, such as white hat hackers or adversarial testing?

Yes. When ES&S determines through a risk assessment that a vulnerability communicated to it from other sources applies to its products and warrants a software patch or update, it uses the established EAC process to develop ECOs, patches or updates and ES&S makes notifications where appropriate following EAC guidelines.

b. Are there vulnerabilities ES&S's is aware of that have not been disclosed to either its customers or the EAC?

All vulnerabilities communicated to ES&S are analyzed for risk and applicability to its software and systems. Not all vulnerabilities are the same. Some vulnerabilities communicated to ES&S apply to commercial off-the-shelf (COTS) software and may not apply to ES&S systems because of the custom hardened configurations the company uses. Other vulnerabilities communicated to ES&S are determined to be so low in severity and low risk of exploitation that it advises customers to maintain current compensating controls to control those. Any vulnerability that meets the EAC reporting requirements is reported.

c. Please provide a list of discovered vulnerabilities, known failures, and malfunctions from the 2016 election until today that have been mitigated and how they were addressed by ES&S. Please also provide the number of discovered vulnerabilities, known failures, and malfunctions that have not been mitigated.

EAC voting system certification includes the testing of any known defect or reported failure that has been identified as requiring a software correction or enhancement. Should the committee wish to review this detailed information, including technical data packages and any other proprietary information, ES&S can arrange to share the requested information under appropriate confidentiality protections.

Election Equipment that is Not Federally Certified

18. Election critical infrastructure includes more than the machines upon which voters cast and count ballots. It includes voter registration databases, election night reporting system, and electronic poll books, for example. While voting systems can be tested and certified by the EAC, these other technologies are not reviewed and certified by the EAC. For ES&S's election products that are not voting systems, including those it manufactures and those that it sells or markets as companion products to its voting machines, how is ES&S ensuring that these products are safe, secure, and up-to-date and utilize current security best practices? How does ES&S check to ensure that its security best practices are effectively warding off attacks?

ES&S' current companion products (voter registration databases and electronic pollbooks) use role-based security, strong encryption of data at rest, strong encryption of data in transit, two-factor authentication and current operating systems supported by their respective vendors.

Additionally, ES&S is a member of the IT-ISAC and MS-ISAC and participates in information sharing to identify potential threats not only to its own systems, but to other members of the IT-ISAC and MS-ISAC as well. All current companion products deployed by ES&S provide for anti-malware, host-based intrusion detection/prevention and network-based intrusion detection/prevention where applicable. ES&S participates in DHS' cyber hygiene program and was the first elections vendor to deploy CIS Albert sensors to monitor real-time threats to its hosted voter registration systems. ES&S systems are also monitored by active firewalls and intrusion detection/prevention systems.

As noted in ES&S' testimony, the company supports increased oversight and testing of voter registration systems and pollbook products.

Network Capabilities

19. What voting machines does ES&S sell that currently have network capabilities (e.g. WiFi capabilities or Ethernet Ports) installed or as an optional add-on? Please provide the names of the machines and the type of network capabilities.

Where requested and authorized by state election authorities, certain ES&S tabulation systems support the transmission of encrypted unofficial results data through a private, secure wireless network. ES&S adds an extra layer of security using an industry-standard Secure File Transfer Protocol (SFTP). The SFTP, which is used by many Fortune 500 companies, establishes an authenticated and secure connection between the DS200 and the central site communications host, allowing encrypted and digitally-signed unofficial results to be securely transferred to the central reporting location after polls close.

This results transmission methodology, which employs the latest technology and most secure features offered by wireless carrier providers, does not use the public internet and is isolated from all public networks, virtually eliminating security risks associated with malware, viruses, spyware, worms and denial of service attacks.

This optional results transmission methodology is for unofficial results reporting only. This transfer of unofficial election results between the DS200 and back-end central reporting location happens after the polls close. Official results are obtained through a manual upload to the Election Management System and canvas performed by election officials at the central reporting location.

20. Is it possible for states to purchase those devices without the network capabilities?

Yes. The standard configuration for the DS200 does not include the ability to transmit unofficial results.

21. What steps does ES&S take to secure its voting systems from the risks associated with a network connection?

ES&S voting systems are designed and built with multiple layers of protection, including physical controls, system hardening and data integrity validation. Each system generates a detailed audit log of all actions and events that have occurred on the unit for post-election review.

ES&S products employ AES-256 encryption standard and digital signatures for all data-in-transit using industry-standard cryptographic modules that have been validated by the NIST Cryptographic Module Validation Program (CMVP).

Each DS200 configured with modeming technology is assigned unique and election-specific credentials that must pass validation parameters when connecting and authenticating with the back-end communications host. Additionally, the communications host is configured to meet the requirements of the FIPS 140-2 standard and provides an additional layer of encryption during the transfer. This transfer of unofficial election results between the DS200 and back-end central reporting location happens after the polls close.

The DS200's optional wireless, secure modem is only activated after polls close, and results are printed from each DS200 on election night. When user credentials are authenticated, an outbound point-to-point secure and private connection is established between the DS200 and the back-end communications host. Once this secure and private connection has been established, a small, encrypted and digitally-signed unofficial election results bundle is transferred to the back-end communications host at the central reporting location. This file transfer takes only a few seconds, and once complete, the modem returns to a deactivated status.

Voting System Certification

22. If ES&S does sell machines with network capabilities installed or as an optional add-on, given the risks of network capabilities, why does ES&S continue to sell machines with this capability? What does ES&S think is its responsibility to notify the customers about the risks of having network capability?

    There are a certain number of states that legally allow for and require the transmission of unofficial results on election night for a variety of reasons, including logistics, density, safety and expedience in reporting. Many of these states and customers have employed this practice for over 25 years. They have requested that ES&S provide this practice in a highly secure and reliable manner with adequate safeguards that do not put their elections at risk.

    ES&S works in partnership with these states' voting system certification bodies, accredited VSTLs, ES&S' security and telecommunications solutions partners and other independent accredited test labs to ensure the company's end-to-end configuration meets the latest cybersecurity protections and best practices.

    ES&S' customers understand the responsibility they have in maintaining highly secure voting system environments. In addition, each customer is provided with a System Security Specification and best practices for maintaining the highest levels of security.

23. Despite the fact that in 2015 the EAC updated the Voluntary Voting System Guidelines (VVSG) by issuing VVSG 1.1, all of the voting systems that Dominion currently sells are certified to a fifteen-year-old standard, the VVSG 1.0. Why does Dominion choose to certify its voting systems to VVSG 1.0 rather than VVSG 1.1?

    While this question is directed at a different manufacturer, ES&S believes that you meant to address it to ES&S as well and, as such, is responding.

    Because the VVSG 1.1 languished without receiving approval for an extended time (due to the lack of a quorum of EAC commissioners), and because the VVSG 1.1 lacked any security-focused enhancements, ES&S, like the other voting system manufacturers, chose to focus its development efforts toward supporting the creation of the 2.0 standards and aligning its system design and development efforts toward its adoption.

24. When ES&S sells add-on components to its EAC-certified systems that are not EAC-certified, what steps does it take to ensure its customers know those components are not EAC-certified? Does ES&S clarify this on its marketing materials? If not, why not?

    ES&S strives to be transparent and forthright in all communications. In the past, ES&S at times referenced optional ("add-on") components in connection to a certified solution. ES&S received notice that referencing optional components might be misinterpreted as part of the certified configuration. Upon receiving this notice, ES&S immediately removed optional component references from marketing materials. To protect against any possible misinterpretation of EAC certified components as opposed to those that may only be state-approved, ES&S added a statement to applicable go-forward materials to direct the reader to a resource with detailed certification information.

25. Once the VVSG 2.0 is in place, how long will it take ES&S to design and develop systems that meet those standards? Is it possible for ES&S to take steps now to prepare for the VVSG 2.0 to minimize the time lag?

ES&S estimates the transition to VVSG 2.0 will be approximately18-36 months from adoption to initial approval. ES&S has maintained regular participation in the Technical Guidance Development Committee (TGDC) working groups to allow it to stay abreast of the emerging standards and align any new development toward any new requirements as they became closer to being final.

Adversarial Testing

26. What adversarial testing does ES&S perform on its voting systems? Please provide details and examples, including a list of the versions of the voting systems ES&S is currently selling that have gone through third-party adversarial testing.

As standard procedure for each release, ES&S' internal security team conducts thorough and pervasive penetration testing of its hardware and software, using the same tools that hackers might use to make sure ES&S' equipment is secure before it ever reaches the customer. After the 2016 election, to complement the company's testing, ES&S submitted its current hardware to third-party security research firms to independently verify the security of ES&S devices.

In March 2018, ES&S submitted its full end-to-end voting configuration of software and hardware for testing by the Idaho National Laboratory (INL), the nation's leading center for research and development in energy, national security, science and environment. These penetration testing efforts allow the company to improve existing security controls already present in ES&S products and adopt new security measures where appropriate. As an example, the company now uses Windows BitLocker on ES&S equipment, implemented industry-leading encryption modules, and locked down internal memory to prevent tampering, among other measures. ES&S' internal security team conducts periodic IT security risk assessments and penetration testing of its corporate network using the same tools that hackers might use to make sure the company's networks are secure.

27. Without providing details about specific vulnerabilities in ES&S's system, what can ES&S share about what it has learned from adversarial testing?

As a result of these testing efforts, ES&S implemented the following improvements to its corporate infrastructure: ES&S contracted with DHS to conduct cyber-hygiene scans of its public-facing internet presence. ES&S signed up with the EI-ISAC to install and monitor five Albert monitors in the voter registration environments it hosts for states and territories. ES&S now receives and incorporates weekly updates from the MS-ISAC on threatening IP and suspicious scanning activity. ES&S uses third-party security monitoring of its corporate network environment. ES&S upgraded the corporate network infrastructure to the latest versions of hardware and operating systems, enabling rapid patching, monitoring and support by equipment manufacturers. Finally, the company also implemented network segmentation to isolate the development, test and quality assurance domains from the production network, among other measures.

28. In addition to the adversarial testing ES&S has performed on its systems, there are independent election security researchers that test its voting systems. In the Coordinated Vulnerability Disclosure Program white paper, ES&S and other vendors in the industry indicated a desire to "vet" researchers.[3]

a. Some have said the industry's desire to place limitations on who can test its systems calls into question its commitment to truly open-ended public vulnerability testing. How does ES&S respond?

ES&S is committed to ethical hacking and is working closely with other members of the election industry and special interest groups to help coordinate and establish the nation's first Coordinated Vulnerability Disclosure Program for election systems.

b. Has ES&S ever taken steps, such as threatening legal action, to try to prevent independent researchers from testing or gaining access to its products? If so, please provide details and explain why ES&S wants to prevent this testing.

ES&S has never threatened legal action in an attempt to prevent independent researchers from testing or gaining access to its products. As a security measure, in 2017, ES&S did advise its customers that in accordance with license agreements, it is not legal to transfer the use of its software or firmware unless the software or firmware have been properly licensed to the new owner of the customer's previously owned voting equipment.

[3] *Coordinated Vulnerability Disclosure Program White Paper*, page 3, available at: https://docs.wixstatic.com/ugd/b8fa6c_112b6b0bdc764533816b57dfdb3481b9.pdf

c. Is it ES&S's position that the modification, execution, possession, or transfer of its elections systems software by an individual without its consent using otherwise lawfully possessed or owned election systems hardware is a copyright infringement?

Yes. ES&S owns the copyright for all its proprietary software and firmware products. ES&S maintains numerous federal copyright registrations on its proprietary software and firmware products. ES&S licenses the use of its proprietary software and firmware products to customers through written license agreements that prohibit the use, display, loan, publication, transfer of possession, sublicensure or other dissemination to or by any third party without ES&S' prior written consent.

Revenue and Investment

29. What percentage of ES&S's revenue in fiscal years 2019, 2018, and 2017 did it invest in research and development? Please provide the percentage by year.

For fiscal years 2017 to 2019, R&D spending averaged 19 percent per year. R&D spending as a percentage of revenue varies each year due to varying revenues year over year.

30. Taxpayer dollars are used to purchase ES&S's voting machines. It is important for taxpayers to know how the investment in research and development compares with the compensation of ES&S's executives. How much money in fiscal years 2019, 2018, and 2017 went to compensating senior management? What percentage of ES&S's revenue did that constitute?

ES&S is a privately-owned company and does not disclose the compensation of any of its employees.

31. During the hearing, Mr. Burt confirmed that ES&S has private equity investors. What role does ES&S's private equity investors play in the direction setting of ES&S's policies and procedures?

No one at McCarthy Group directs ES&S management regarding the company's operations. ES&S' board acts as a governing board, not a working or managing board.

Paper Records in Voting

32. ES&S has committed to no longer sell paperless machines, but it appears to be selling the ExpressVote with an "Autocast" feature that allows voters to skip the verification of the paper record. Although Mr. Burt testified that no customers are using that feature, it is still something that ES&S advertises and sells. How does ES&S know that no customers are using this feature? Given that a primary criticism of paperless machines is that they did not have a voter verified paper audit trail, does the continuing sale and marketing of a

feature that can record votes without a voter verified paper trail comport with ES&S's commitment to stop selling paperless machines?

All current ExpressVote offerings allow the voter the option to review his or her printed selections by ejecting the paper record from the ExpressVote before reinserting the paper and casting his or her ballot. "Autocast" was a feature whereby the voter was not given the choice to review his or her printed selections before casting the ballot. The original intent of this feature was to streamline the voting process for those individuals who are physically unable to handle a paper ballot. A review of ES&S' records indicates that no customer has used or is currently using this feature. In other words, all jurisdictions using the ExpressVote provide the voter with the option of ejecting the paper record for review. The unused "Autocast" feature has since been removed from the current versions of ES&S voting systems, starting with version EVS 6.0.4.0, federally certified in May 2019, and is aligned with ES&S' decision to no longer sell paperless voting machines as the primary voting device in a jurisdiction.

Lobbying and Influence

33. Mr. Burt testified that ES&S has a policy that every one of its employees, "Vice President and above, as well as anyone engaged in sales and marketing activities," are "strictly prohibited" from making campaign contributions.

a. Please provide the ES&S policy governing campaign spending and/or campaign contributions.

See the attached policy.

b. What are the policy's effective dates, and is it still in effect?

The policy has been in effect since 2004 and has been updated over time.

c. To whom does the policy apply?

See the attached policy.

d. Does the policy cover corporate contributions?

See the attached policy.

e. Does the policy cover employee contributions?

See the attached policy.

f. Does the policy cover those with whom ES&S contracts?

See the attached policy.

g. Mr. Burt indicated that the policy does not apply to lobbyists. Does this mean the policy does not apply to lobbyists at the federal, state, and local levels?

Yes.

h. What policies, if any, does ES&S have governing contributions to organizations organized under 26 U.S.C. § 527 (a "527 group")? Has ES&S made any contributions to a 527 group? If so, please provide the dates, recipients, and amounts.

Upon request, ES&S has in the past sponsored events for Secretaries of State hosted by the RSLC and the DCEC just as it annually sponsors events held by the National Association of Secretaries of States. Our records indicate the following sponsorships:

Date	Donation
11/2008	$300
11/2013	$7,500
10/2014	$7,500
10/2015	$10,000
10/2016	$10,000
9/2017	$3,000
8/2018	$3,000

i. What policies, if any, does ES&S have governing contributions to nonprofit organizations, including membership associations? Has ES&S made any contributions to such organizations? If so, please provide the dates, recipients, and amounts since 2010 and the purpose of the contributions.

ES&S supports the work of various local philanthropic charitable organizations through sponsorship and attendance at various fundraising events conducted by such organizations.

j. How are these policies enforced?

As stated in the Policy, violations of the same could subject an associate to termination of employment. ES&S closely monitors the activities of the company and its associates to ensure compliance with the Policy.

34. Concerning ES&S's lobbying and marketing practices and policies:

a. What percentage of ES&S's budget was spent on lobbying in fiscal years 2019, 2018, and 2017? How much money did that constitute in dollar figures? How are those funds spent?

Fiscal Year	Dollar Amount	Use of Funds
2019	$2,461,523	Voting System Sales and Support Activities
2018	$2,278,576	Voting System Sales and Support Activities
2017	$2,303,560	Voting System Sales and Support Activities

b. What percentage of ES&S's budget was spent on marketing in fiscal years 2019, 2018, and 2017? How much money did that constitute in dollar figures? How are those funds spent?

Fiscal Year	Dollar Amount	Use of Funds
2019	$669,245	Marketing Materials; Conferences; Sales Demonstrations
2018	$655,854	Marketing Materials; Conferences; Sales Demonstrations
2017	$599,741	Marketing Materials; Conferences; Sales Demonstrations

c. Please provide a list of jurisdictions in which ES&S has registered lobbyists.

Current as of the writing of this response - Arkansas, California, Delaware, Florida, Illinois, Indiana, Kentucky, Louisiana, Maryland, Minnesota, Missouri, New Jersey, New York, North Carolina, Ohio, Pennsylvania, South Carolina, Tennessee, Texas, Virginia, Washington, D.C.

35. A June 2018 McClatchy article, described an ES&S practice of maintaining a "Board of Advisors," comprised of election officials that are responsible for negotiating and awarding voting system contracts.[4]

a. Does ES&S continue to maintain a "Board of Advisors" comprised of election officials that are responsible for negotiating and awarding voting system contracts or a similarly structured board?

[4] Greg Gordon, et al. "Voting machine vendor treated election officials to trips to Vegas, elsewhere," *McClatchy* (June 21, 2018) https://www.mcclatchydc.com/latest-news/article213558729.html.

Members of the ES&S advisory board, which has not been in existence since early 2018, consisted of a small group of customers who were current users of ES&S technology. Board members historically recused themselves from the board when their jurisdiction had an open procurement for voting systems. Some customers did not return to the board because they bought products from other suppliers. At no time did ES&S have advisory board members who were prospective customers or non-customers. Rather, only existing customers were on the board.

b. Please provide a list of all past and present "Board of Advisors" members.

This information should be disclosed by the former members. There are no present members, and there have been no meetings for the last two years. The advisory board is no longer in existence.

c. Does ES&S pay for travel and entertainment for the Board of Advisors to attend meetings about ES&S products? Please provide details.

The ES&S advisory board provided members the opportunity to hear each others' perspectives on voter and elections administrator needs, to share best practices, and to learn about federal updates. For example, a meeting held in 2017 included the U.S. Department of Homeland Security discussing elections as critical infrastructure. Board meetings were filled with technical and operational information sharing. Board members historically consulted with their state or county ethics boards regarding travel expenses. Some board members covered their own expenses.

Unsigned Code

36. In response to Chairperson Lofgren's question: "Do all of your election systems currently in use prevent unauthorized code or altered operating systems from running on them in this way?" Mr. Burt responded: "They do, Chairperson." However, the 2019 DEFCON Voting Village Report indicated that the ES&S ExpressPoll electronic poll book had secure boot disabled and would boot arbitrary, unsigned operating systems, which would also allow unsigned code to run. The report also stated that ES&S Automark allowed for running arbitrary, unsigned software after using a keyboard to exit the voting program. In 2018, the DEFCON Voting Village Report indicated that the ES&S M650 would run arbitrary, unsigned code loaded on its Zip disks. And finally, according to a 2018 New York Times story, ES&S submitted to California for certification in 2017 an optical scanner that would run arbitrary, unsigned code installed on it.[5] The cybersecurity

[5] Kim Zetter, The Myth of the Hacker-Proof Voting Machine, *N.Y. Times Magazine* (Feb. 21, 2018), https://www.nytimes.com/2018/02/21/magazine/the-myth-of-the-hacker-proof-voting-machine.html.

researcher who made the discovery stated that the machine either had no code authentication or its code authentication was broken.

a. Given these examples of ES&S election systems currently in use lacking protection against the running of unsigned code or altered operating systems, does Mr. Burt have any clarification for the Committee?

All systems referenced in this question are aged systems that are no longer manufactured by ES&S. All current ES&S systems employ protections against the running of arbitrary code or altering of operating systems. As just one example, the current ExpressPoll electronic pollbook does use both Secure Boot as well as Microsoft's BitLocker technology to prevent unsigned operating systems, as well as protecting all data on the electronic pollbook with strong encryption.

b. Mr. Burt also stated that: "The memory stick that we purchased from a U.S. manufacturer, our election management system won't even operate unless they know that it's a particular serialized number memory stick." Can ES&S confirm that even in the instance where someone was able to install unsigned code onto these machines, either through a flaw in verifying the "memory stick" or some other means, that these machines would prevent that unsigned code from executing?

Yes. The DS200 checks all files it uses on the memory stick and digital signatures before using them. If one is not correct, the DS200 will stop functioning and report on screen an invalid signature was found.

c. Can ES&S please provide to the Committee a whitepaper or more technical description of how exactly your unsigned code protection works? Disclosure of such details is common practice among computer and smartphone vendors, who have both publicly disclosed technical details of how their secure boot and code signing protections work.

ES&S does not have a white paper available at the current time. Should ES&S produce one, the company will make it available on the ES&S website for public consumption.

Remote Access

37. During the hearing, Mr. Burt testified that none of the ES&S machines currently in use in the country had remote access installed. How has ES&S confirmed that remote access software is no longer present or in use in any of its voting systems?

Yes, ES&S can confirm that there is no remote access software in any of the company's voting machines. A detailed review of customer records confirms that fact.

For the record; Between 2000 and 2006, about three percent of jurisdictions across the U.S. received licenses for remote technical support on county workstations. This software was never designed to and did not come in contact with any voting machines. It was only provided upon customer request, and very few customers chose to install it. The limited number of users began to discontinue and uninstall the software as they migrated to newer EAC certifications and requirements, which were adopted in 2007. This software is no longer installed, nor has it been in use for several years.

MINORITY QUESTIONS FOR THE RECORD

1. Could you describe in detail how some of your machines are able to assist voters with disabilities?

ES&S is serious about accurately capturing the intent of every voter. ES&S strictly follows the guidelines set by the ADA to ensure voting on its machines provides a simple, private and inclusive voting experience.

The ES&S ExpressVote family of products, including the ExpressVote and ExpressVote XL Universal Voting Systems, has received high praise for the inclusiveness it brings to the election process. Both voting machines can be configured in several ways to serve every voter as fully compliant ADA voting solution during early voting and on Election Day. On an ES&S Universal Voting System, EVERYONE votes in the same private and independent manner.

ES&S follows all ADA requirements and works with voters with disabilities, as well as advocates and experts in the field of accessibility, to test its equipment first hand. This valuable feedback helps guide the company's product development teams, and in turn, ensures EVERY voter can exercise his or her constitutional right to vote with anonymity on a universal voting system. To protect voter privacy, the printed paper record does not specify whether assistive devices were used to conduct a voting session.

The ES&S ExpressVote and ExpressVote XL include the following accessibility features:

- Seated- and standing-height configurations to serve both seated and standing voters
- Adjustable on-screen high contrast and zoom functionality display settings to make the on-screen text more readable
- Audio ballots in voters' selected language
- Audio ballot option for visually impaired voters as well as voters with a disability or special need
- Screen prompts, symbols and audio to help voters navigate the vote selection process
- Assistive technology connections and devices
- Voter's option to blank the screen for privacy
- Voters can verify the printed paper record accurately captured their selections using the same accessible device

The ES&S ExpressVote family of products provide all voters, regardless of limitations, with the option to navigate ballot selections independently using various ADA support peripherals including, but not limited to:

- Headphones
- Audio-tactile keypad with Braille legends
- Sip-and-puff device
- Two-position rocker switch

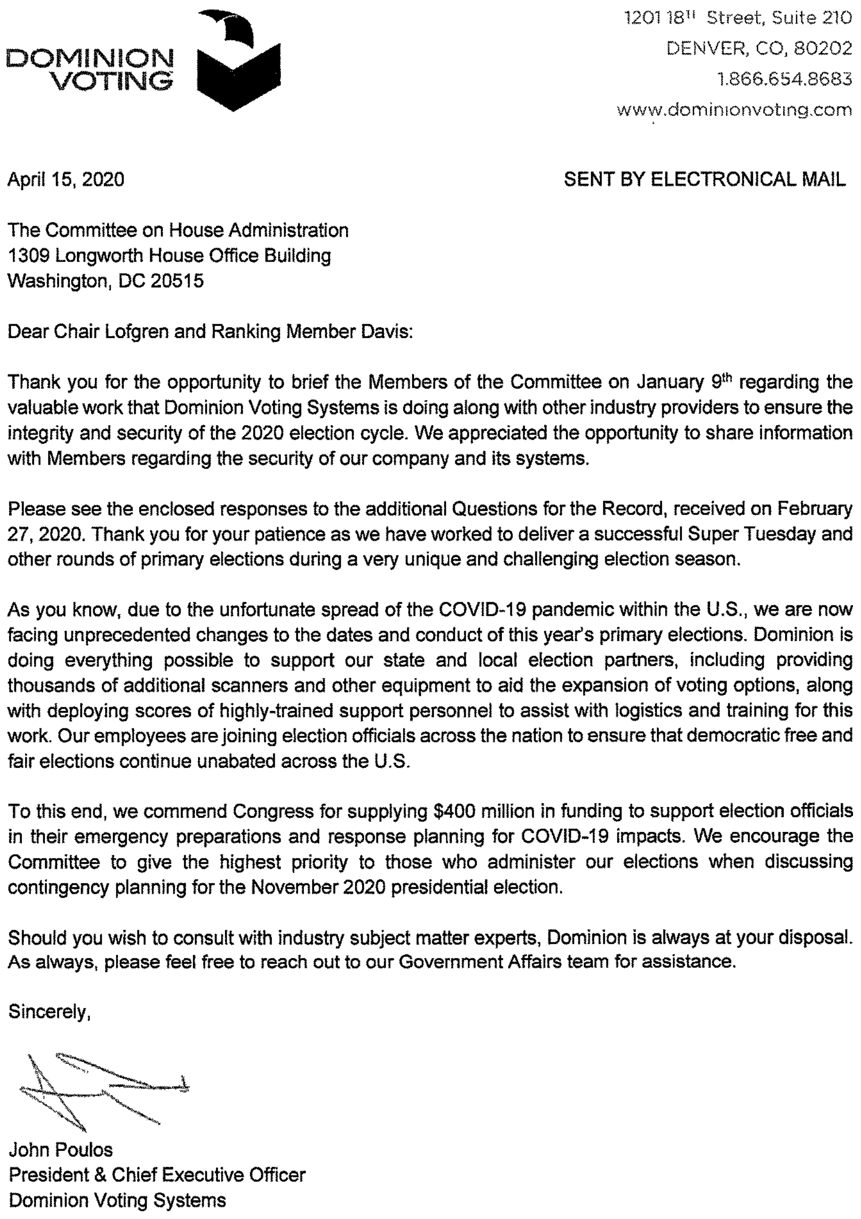
POLITICAL CONTRIBUTIONS

ES&S is in the business of supporting democracy worldwide through its provision of election products and services throughout the U.S. and abroad and encourages its Associates to stay well informed regarding local, state, and national affairs and to vote in elections. It is imperative, however, that ES&S and its Associates maintain and continuously convey a neutral, apolitical business environment in all of ES&S' business dealings.

ES&S and its Associates are strictly forbidden from engaging in politics, endorsing political candidates or parties, or making any political contributions for or on behalf of ES&S.

In addition, subject to applicable law, Associates are strictly forbidden from directly or indirectly endorsing political candidates or parties, running for or holding political office, or making political contributions to any candidates, political parties, election issues, or causes.

The Associate should immediately contact the Human Resources Department or their Manager for more information or regarding political contributions or support.



DOMINION
VOTING

1201 18th Street, Suite 210
DENVER, CO, 80202
1.866.654.8683
www.dominionvoting.com

April 15, 2020

SENT BY ELECTRONICAL MAIL

The Committee on House Administration
1309 Longworth House Office Building
Washington, DC 20515

Dear Chair Lofgren and Ranking Member Davis:

Thank you for the opportunity to brief the Members of the Committee on January 9th regarding the valuable work that Dominion Voting Systems is doing along with other industry providers to ensure the integrity and security of the 2020 election cycle. We appreciated the opportunity to share information with Members regarding the security of our company and its systems.

Please see the enclosed responses to the additional Questions for the Record, received on February 27, 2020. Thank you for your patience as we have worked to deliver a successful Super Tuesday and other rounds of primary elections during a very unique and challenging election season.

As you know, due to the unfortunate spread of the COVID-19 pandemic within the U.S., we are now facing unprecedented changes to the dates and conduct of this year's primary elections. Dominion is doing everything possible to support our state and local election partners, including providing thousands of additional scanners and other equipment to aid the expansion of voting options, along with deploying scores of highly-trained support personnel to assist with logistics and training for this work. Our employees are joining election officials across the nation to ensure that democratic free and fair elections continue unabated across the U.S.

To this end, we commend Congress for supplying $400 million in funding to support election officials in their emergency preparations and response planning for COVID-19 impacts. We encourage the Committee to give the highest priority to those who administer our elections when discussing contingency planning for the November 2020 presidential election.

Should you wish to consult with industry subject matter experts, Dominion is always at your disposal. As always, please feel free to reach out to our Government Affairs team for assistance.

Sincerely,

John Poulos
President & Chief Executive Officer
Dominion Voting Systems

Responses by Mr. John Poulos, President and CEO, Dominion Voting Systems
Questions for the Record following the January 9, 2020 Hearing
Committee on House Administration, "2020 Election-Security Perspectives from Voting System Vendors and Experts"

Questions Submitted February 27, 2020
Responses Submitted April 15, 2020

NOTE: The spelling of Mr. Poulos' name has been corrected throughout the document for the record.

1. During the testimony of Mr. Poulos, he testified he would support federal reporting requirements specified below. Please provide the following information to the Committee:

   a. Dominion's cybersecurity practices, including incident response procedures.

   As noted in Mr. Poulos' written testimony, "Consistent with our founding tenants, Dominion works hard to promote a company culture of security. This includes annual, mandatory background checks and cybersecurity awareness training for all employees. Dominion is committed to investing in security and innovation efforts, tracking risk and threat information, developing new capabilities and successfully supporting our customers."

   "Dominion has also adopted advanced digital protections while employing a Defense-in-Depth approach to our internal infrastructure. Multiple layers of protection are in place spanning user endpoints, network and systems infrastructure and cloud systems, along with multi-factor authentication. We conduct continuous vulnerability scanning on our company network and utilize third-party services for threat hunting and breach detection. Specifically, we have implemented email verification records for Sender Policy Framework ("SPF"), DomainKeys Identified Mail ("DKIM"), and Domain-based Message Authentication ("DMARC") to protect communications with associates and customers."

   "Dominion actively engages with the U.S. Department of Homeland Security ("DHS") and other trusted, third-party advisors to enhance and maintain our physical and cyber security posture. In addition to mandatory state and local disclosures for confirmed or suspected breaches and incidents, we also adhere to the EAC's mandatory requirements for reporting system issues in federal elections.[1] Together with federal, state and local government partners – as well as other industry counterparts, we conduct coordinated emergency drills, tabletop exercises and routine information-sharing as a member of the DHS Sector Coordinating Council for Election Infrastructure. Through these efforts, Dominion has refined our company's situational awareness and strengthened our procedures for handling a wide variety of incidents and emergencies, including cyber attacks. We also conduct briefings and training sessions with state and local election officials who use our systems to educate and inform them of best practices for securing their voting equipment and chain of custody process."

[1] See *EAC Testing & Certification Program Manual Version 2.0*, https: www.eac.gov/assets/1/6/Cert_Manual_7_8_15_FINAL.pdf

For cyber incidents, we adhere to the general guidance contained in the DHS "Incident Handling Overview for Election Officials," which outlines best practices for documenting and responding to cyber-related incidents. The company takes an Incident Response Team approach and retains various partners to support Election Day operations, as needed. We hold active membership status in two separate ISACs for information-sharing: the IT-ISAC and the EI-ISAC. Finally, we participate in the DHS Election Day "Ops Room," most recently opened for Super Tuesday.

b. Any cyberattacks Dominion has experienced. This should include any phishing attempts Dominion has detected.

As Mr. Poulos stated during the Committee's January 9th hearing under questioning, Dominion experienced no major or reportable company incidents, breaches or cyber attacks in 2016, nor at any time since. We continue to be vigilant and partner with CISA and state government partners on tabletop planning and response exercises, having recently taken part in the national "Tabletop the Vote" emergency planning exercise in February 2020. Company employees undergo mandatory cybersecurity awareness training to learn how to deal with phishing emails in a secure and effective manner. More recently, we have seen periods of increased cyber activity against company networks – including regular phishing attempts – and disinformation involving our company/voting systems on social media, consistent with peak periods for a major election cycle.

c. Personnel policies and procedures, including whether background checks and other procedures are in place to safeguard against inside attacks and how Dominion assesses current employees on an ongoing basis for security risks. Please specify the policies and procedures.

As noted by Mr. Poulos during the January 9th hearing, all new company hires undergo a background screening that includes a criminal history check and a credit history review. We also employ other internal practices to maintain the security of our company and its personnel, facilities and products. The following checks are done on an annual basis, if and when compliant with various State laws and regulations:

- Social Security number trace
- Seven-year county criminal search
- Seven-year federal criminal search
- Enhanced nationwide criminal search
- Fifty-State sex-offender registry search
- OFAC/ Terrorist Watch List / FBI Most Wanted / Interpol
- Credit check
- Motor Vehicle check

d. Details of corporate ownership and foreign investment. Please submit a list of all individuals and entities with a five percent or more ownership or control interest in Dominion, including private equity investors, and indicate the percentage of ownership or controlling interest. Please also provide a list of all investment by foreign entities and individuals in Dominion.

Dominion ownership of greater than 5% is as follows:

- Staple Street Capital Group, LLC – 75.2% (US-based company with New York City office)
- Mr. John Poulos, President and CEO/Co-founder – 12.4% (Canadian citizen)
- Except for Mr. Poulos (FVEY nation) citizens, there are no other investment by foreign entities and individuals in Dominion. Additionally, Mr. Poulos underwent a CFIUS review prior to any investment.

Dominion has also shared with Congress some other important disclosures that are routine for voting system providers but are not mandatory for any other election tech providers (such as e-pollbook, voter registration, and voter information tool vendors), including:

- Notify all U.S. customers of business change of ownership/control or change of IRS "responsible party" disclosure designation
- Maintain up-to-date manufacturer registration information with U.S. Election Assistance Commission ["EAC"]
- Attest that the company:
    - Has not/will not be acquired by persons on the Specially Designated Nationals and Blocked Persons List published by the U.S. Office of Foreign Assets Control (OFAC)
    - Has not/will not be acquired by persons convicted of a cyber-crime, election offense or charge of election fraud in the U.S. or abroad
    - Has not/will not be acquired by foreign persons listed or otherwise implicated under Executive Order 13757 (December 28, 2016), "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities"

e. Details on Dominion's supply chain, including where parts, software patches, and installations come from; how are they transported; and how they are kept secure.

As Mr. Poulos noted in his testimony before the Committee, Dominion remains fully committed to protecting the integrity of elections. All of our programming work is done in-house by Dominion employees. We use vetted partners in our manufacturing supply chain. All systems have undergone thousands of hours of quality review and internal performance testing before systems and software components are supplied to the federal government for Voting Systems Test Lab inspection.

In response to the Committee's previous inquiry to Dominion in October 2019, under the EAC Testing & Certification Program vendors are required to submit complete listings of software and hardware (BOM) components in a Technical Data Package (TDP) to the VSTL for each voting system to be tested. The TDP must provide enough data so that the VSTL can unequivocally identify the software and hardware components of the system configuration submitted for testing, along with descriptions of how they are assembled and used in the operation and maintenance of the system. Further, every unit is given a serial number for tracking purposes.

This information should be available to the Committee with proper protections in place for sharing company-sensitive information.

Efforts to secure our supply chain also include:

- Protection of manufacturing operations
- Management of component suppliers
- Policies on secure coding practices
- Tracking inventory
- Secure container protocols for products in transit
- Monitoring of risks to technology and data
- The use of custom tamper-evident seals designed for customer shipping/use

Because we recognize our partner role with customers in securing our supply chain, Dominion also routinely provides training services and education to local jurisdictions, which includes equipment-handling and general storage security recommendations upon delivery.

2. In addition to reporting the information above discussed during the hearing, please provide the following information to the Committee. This is all information that Dominion is required to provide to at least one of the states in which its machines are certified:

a. Management and staff organization; number of full-time employees by category; and number of part-time employees by category.

Dominion currently employs 261 FTEs and 3 PTEs.

b. Financial history of the business, including a financial statement for the past three fiscal years.

Well-established process allows U.S. voting systems manufacturers to lawfully and securely disclose financial information with state and local election authorities, exempt from public information requests or with a non-disclosure agreement in place to prevent company harms. Dominion is willing to share information with the Committee with a similar arrangement in place.

c. History and description of the business, including year established; products and services offered; states with machines Dominion's manufactures or services; branch offices and subsidiary and/or parent companies.

Dominion was established in 2003, as noted by our CEO and co-founder John Poulos during the January 9th hearing. In addition to our Denver main office, the company has branch offices in six locations across the U.S. Additional information about the company, its founding, our products and our customers, can be found at: www.dominionvoting.com.

d. Audited report of the business' fiscal year 2019.

Please see answer to question 2 (b).

3. During the January 9, 2020, hearing, Mr. Poulos could not provide the Committee with the precise percentage of components from China on the spot. For all the questions below, please also provide specifics on the relevant components by describing them; whether they are inert or programmed or programmable; and the machines for which those components are used.

    a. Please provide the percentage of the components in Dominion's supply chain that come from China.

    b. Please also provide the percentage of components in Dominion's supply chain that come from foreign countries other than China. Please provide the country and percentages by country.

    c. Please provide the percentage of components come from China-based companies.

    d. Please provide the percentage of suppliers in Dominion's supply chain that have locations in either China or Russia.

    For systems manufactured by Dominion, the percentage of electronics parts programmed outside of the U.S. ranges from 0.16 percent to 0.7 percent. These parts are sourced from a publicly-traded, U.S.-based company.

    We can assure the Committee that Dominion does not source any parts or components from Russia. As noted during the hearing, some of the components sourced from China would be difficult or impossible to find elsewhere. The industry's joint statement on supply chain security in December 2019 cautioned, "[T]he practice of assessing risk based solely - or even primarily - on the geography of a supplier's corporate locations is a practice that has been widely discredited. Supply chain risks and threats exist regardless of where a company is located, or where its products are manufactured or assembled."

    For 2020 and beyond, we are working closely with CISA and other stakeholders to identify additional tools and best practices for assessing risks in voting system supply chains. As Mr. Poulos stated in his written testimony to the Committee, more actionable intelligence on this subject from DHS and other U.S. government intelligence partners is also sought. Specifically, he remarked, "increased transparency around malign activity observed by intelligence agencies... would go a long way towards enabling private sector election providers to better prioritize resource allocations in the same economic terms as other enterprise decisions."

4. In addition to concerns about the components in Dominion's supply chain, the Committee requests more information on Dominion's software development.

    a. Where is Dominion's firmware and software developed? If it is developed in multiple locations, please specify those locations.

Dominion maintains an office in Toronto, Canada, where our in-house engineering and development teams are headquartered. We are currently in the process of migrating a small number of full-time employees based outside of North America to our Toronto office as part of our ongoing company risk identification and mitigation efforts. All Dominion voting systems and software are submitted to the U.S. EAC and federally-certified Voting System Test Labs (VSTLs) for review, testing and certification.

b. Where is it installed?

See previous answer.

c. How does Dominion protect it from remote access and tampering outsiders? Please provide specifics.

All Dominion-manufactured voting systems include the following features:

- Not designed to be connected to the Internet or to public networks
- Can be hardened by turning off ports and services not necessary for the application operation and configuring the BIOS to limit boot vectors (DISA STIG benchmarks).
- Multi-factor authentication
- Permission settings that segregate Operator, Administrator and Technician functions.
- Encryption of data (AES256)
- Digital signatures on election records (SHA-256)
- Comprehensive, non-alterable audit logs
- Tabulators only accept voting software with proper encryption keys
- Tally systems only accept files with proper encryption keys
- Physical security seals and locks

5. For components that are manufactured in other countries, like China and Russia, is it possible for you to find different manufacturers that are in the United States or in countries that have not been accused of committing cyberattacks against the United States? If not, why not? For example, is the component protected by a patent?

As noted by all of the CEOs who testified at the January hearing, voting systems manufacturers would be challenged to source certain product hardware components from outside of China. In some cases, there are simply no alternative suppliers. In other instances, domestic restrictions on point of origin could create economic hardships for manufacturers and their customers, or result in potential production delays or shortages. We are always working to seek out reasonable alternatives, where available.

6. In Dominion's response to the Committee's September 19, 2019 letter asking questions about how Dominion protected the security of its supply chain, Dominion provided some best practices which it follows. How specifically does Dominion know that its best practices are working – if they are – and that its supply chain is secure? What checks does Dominion have in place?

Dominion works closely with our government partners to test and certify our systems for security, accuracy and reliability. They are routinely subjected to rigorous review, analysis, testing and certification by election authorities at the federal, state and local levels. Once the system software is certified, any changes require a new round of testing by election authorities. This process helps to ensure that product vulnerabilities are discovered and addressed before systems are placed into use. We are also working with the National Institutes of Technology (NIST) via a DHS Election Infrastructure Working Group to develop an Election Infrastructure Cybersecurity Profile to help our company and our customers manage associated supply chain risks.

7. Interos wrote on page five of its report Election Technology & the Global Supply Chain that it notified the manufacturer of the machine that was the subject of the report.[2] The report stated that "Interos recognizes the extreme sensitivity of election security matters and has contacted the affected company involved." Has Dominion been notified by Interos that it is the vendor that manufactured the machine discussed in the report?

No. As Mr. Poulos made clear during the January hearing, Dominion is confident that we are not the company whose product was analyzed in the report.

8. What steps does Dominion take, if any, to ensure that subcontractors and manufacturers producing its components overseas are not subject to influence from a foreign government?

All contractors are required to undergo a thorough vetting process. In addition to our own screening methods and checks, Dominion is confident in the ability of our U.S. Federal Intelligence partners to provide accurate and timely nation-state focused threat and intelligence information-sharing regarding supply chain threats. As noted in Mr. Poulos' written testimony submitted to the Committee for the hearing, the company welcomes "continued assistance from our federal partners in evaluating cyber risks for voting technology, to include increased transparency around malign activity observed by intelligence agencies. This would go a long way towards enabling private sector election providers to better prioritize resource allocations in the same economic terms as other enterprise decisions."

9. Studies on the use of ballot marking devices show that voters check their ballots at very low rates and alert election officials to errors at an even lower rate. Is Dominion working to design ballot marking devices or to identify other technical solutions that improve the rate of voter verification of their printed ballots to ensure that there is a reliable voter-verified paper trail from its ballot marking devices that can be audited with confidence?

All Dominion systems provide voters with the important opportunity to review their selections before casting a vote. We work collaboratively with U.S. election administrators to provide a variety of voting systems and methodologies based upon jurisdictional requirements, as well as federal and state certification standards. These methodologies include hand-marked and BMD ballot scanners/tabulators,

[2] *Election Technology & the Global Supply Chain*, Interos, (Dec. 16, 2019), page 5, https://cdn2.hubspot.net/hubfs/5812029/Interos%20-%20Election%20Security%20Paper.pdf

ballot marking devices (with or without the use of QR codes), Voter Verified Paper Audit Trail systems, UOCAVA and others. All systems allow for independent voting by electors with disabilities. The Dominion platform is adaptable and allows election administrators to readily change voting methodology. For example, we are currently working with the Colorado Secretary of State's office to produce an alternative method of printing BMD full face-ballots that does not include QR codes.

Additionally, all Dominion platforms allow for simple and transparent auditing, including Risk-Limiting Audits (RLAs). In 2017, Dominion equipment was used by the State of Colorado in the first-ever statewide RLA conducted in the U.S. The Colorado RLA included BMD ballots with QR codes.

10. Some experts in election security have raised significant concerns about the risk of ballot marking devices that store information about the choice a voter made on their ballot in a non-transparent format, such as a barcode or QR code. During the testimony of Mr. Poulos, he confirmed that Dominion sells equipment that tabulates votes based on a barcode or QR code.

    a. Please specify how Dominion's ballot marking devices tabulate votes.

    b. What steps does Dominion take to ensure that voters can be confident that their choices will be counted accurately?

    c. Has Dominion re-evaluated selling it given these concerns?

    d. Are the barcodes or QR codes used by Dominion's ballot marking device readable by any off the shelf barcode or QR code scanner?

The ImageCast X ballot-marking devices do not tabulate votes. Voters can be confident in the ability of all certified Dominion systems to provide for safe, accurate and reliable elections, knowing that they have gone through a formal testing and approval process for government certification and use. Please see answer to question 9 for additional information.

11. As we discussed during the hearing, the Consumer Product Safety Commission advises manufacturers of consumer products to "identify all reasonably foreseeable hazards associated with" their products and include safety warnings and steps to reduce risk in the user guides. There are similar requirements for motor vehicles and warnings in owner's manuals. During the hearing, Mr. Poulos testified he would support a requirement for voting system vendors to provide guidance to customers identifying security risks associated with use of Dominion's equipment and recommendations to mitigate those risks.

    a. Does Dominion currently include such guidance for election officials buying its products?

    As Mr. Poulos stated during the hearing, our company supports the concept. All system user guides include information for election officials to securely store, maintain and operate their equipment. In addition, testing and certification helps to solidify the types of operating and maintenance procedures that are recommended to customers. We routinely work with the EAC on this subject and urge Congress to utilize the agency for additional information on this topic.

b. If yes, please detail what is included.

See previous answer.

c. If no, isn't it reasonably foreseeable that an election official might need that guidance or warning, particularly in the current threat environment? Why does Dominion choose not to provide such guidance? Does Dominion have any plans to do so in the future?

N/A

d. Does Dominion provide any instructions concerning audits? Does Dominion recommend risk limiting audits?

As Mr. Poulos noted during the hearing, Dominion equipment is fully supportive of risk-limiting audits and other types of post-election auditing, which we support as a best practice for election administration. We always stand ready to assist customers with this process, having gained a great deal of industry expertise on the subject. In 2017, Dominion equipment was used by the State of Colorado in the first-ever risk-limiting auditing conducted in the U.S., which confirmed the high accuracy rates of our system.

e. Given the security concerns around logic and accuracy auto-testing, and the failures that happened in Northampton County, PA in 2019,[3] does Dominion recommend manual logic and accuracy testing for every ballot style? How many of Dominion's machines have an auto testing feature?

Northampton County, Pennsylvania is not presently one of our customer jurisdictions. However, Dominion is highly supportive of manual L&A testing as a way to simulate the true functionality of the entire end-to-end voting system. We have one system that includes an auto-testing function, which allows a jurisdiction to decide whether or not it is used.

f. What other election day support does Dominion provide to its customers? If this varies based on the contract, please provide specifics on the different contracts Dominion has and the support provided in each and the price difference between the levels.

Dominion provides varied levels of Election Day support depending on contractual agreements with customers. This can vary from help desk support to onsite implementation.

12. During the hearing, Mr. Poulos confirmed that Dominion employs a chief information security officer.

[3] Tom Shortall, *No Confidence: Northampton County election board 'extremely disappointed' in machines it selected*, The Morning Call (Dec. 19, 2019), https://www.mcall.com/news/local/mc-nws--20191220-xrkqrrokfrgzlc3lglpn5nf5fe-story.html

a. What is that individual's title?

b. How long have they been on staff?

c. What authority do they have within the company?

d. Does that person hold any other titles or responsibilities within the company?

Dominion has a full team of personnel that is tasked with securing company networks and products, with a regular reporting cadence that flows directly to the Board of Directors. The company employs a Vice President of IT & Security who holds a U.S. Government security clearance. He and his team have the authority for driving security improvements for all IT and corporate network infrastructure, including employee cybersecurity testing and training. He also manages our technical information-sharing with the EI-ISAC and the IT-ISAC. This is his sole title and role within the company.

13. Does Dominion have technical staff with cybersecurity expertise involved in all stages of the product—the marketing, the design, the testing, the service, and support?

Dominion relies upon internal and external experts to provide vital professional engineering, design and security expertise in producing our products and solutions.

14. When Dominion, or someone Dominion contracts with, assists jurisdictions with programming services, how are those files delivered to the jurisdiction? What steps do you take to ensure the transfer and delivery of the programming files is secure? What steps do you take to secure the device the programming actually takes place on?

Dominion takes every step possible to ensure that the transfer and delivery of the files are secure. The company abides by the contractual requirements of customer agreements, pursuant to the laws, processes and certification standards of each state.

15. The Election Assistance Commission (EAC) issued a Notice of Clarification on De Minimis Software Changes in November of 2019.

a. Has the EAC's Notice of Clarification on De Minimis Software Changes made the certification of security updates easier?

The EAC's notice has been helpful at the federal level, but more work is needed to streamline certification pathways for security-related updates. This work should improve with the adoption of the VVSG 2.0 guidelines and the evolution of related processes across the ecosystem.

b. Has that Notice solved the issue with delays to the certification of security updates?

See previous answer.

c. How does Dominion ensure that states receive security updates for their voting systems?

This is done in accordance with federal and state law, as well as customer agreements.

d. On average, once an update is certified, how long does it take for a state to receive that security update?

The timeframe often depends on a variety of factors, including approval by the state election authority under applicable certification standards and permissible practices for the installation of such updates. Dominion routinely makes updates available to our customers, and we strongly encourage their utilization in order to ensure that systems are as up-to-date as possible.[4] We are hopeful that VVSG 2.0 will usher in a faster, more flexible process that allows for the introduction of innovative technologies and incentivizes more effective maintenance of deployed systems to address any documented threats and vulnerabilities which cannot otherwise be remediated through use of compensating personnel, procedural safeguards or physical controls.

e. How is the security update transmitted to the local election officials? What are the costs associated with getting a security update or patch?

This process is arranged with approval by the state election authority under applicable certification standards and permissible practices for the installation of such updates. To the extent that any costs are involved, they will vary based upon the extent of the update and certification processes required.

16. Your company regularly submits updated voting systems to the EAC for certification.

a. Once an updated system is certified, do jurisdictions have the opportunity to update their systems?

Yes, this is covered under licensing agreements and arranged with approval by the state election authority under applicable certification standards.

b. How does this process work? For example, is a physical intervention needed?

Yes, given the closed, embedded security of the hardware.

c. Is the process different if the update is certified by the EAC as a new system versus a modification?

Updates or new system installations are arranged with approval by the state election authority under applicable certification standards and permissible practices for such state.

d. For machines that run a version of Windows that has reached the end of its life, will Dominion provide updates to jurisdictions?

[4] Please note: The decision to utilize manufacturer updates is governed by the controlling jurisdiction.

Yes, with the necessary approval of the state/jurisdiction in question.

e. If so, what will the process be for those updates and will Dominion be charging jurisdictions for those updates?

This process varies greatly by state and local jurisdiction. There is no charge if covered by licensing or maintenance agreement.

17. In Dominion's October 18, 2019 response to the Committee on House Administration's oversight letter, Dominion told the Committee that it is required to "report certain issues (i.e. malfunctions) to the EAC following each federal election."

a. Does Dominion also disclose to its customers and to the EAC vulnerabilities discovered from other sources, such as white hat hackers or adversarial testing?

Yes, the company fully complies with all federal and state laws for such disclosures and reporting. We work with federal, state and other stakeholder groups (i.e. adversarial testers and independent researchers) to identify controls and mitigations together. However, if a product vulnerability is discovered in the prototype or development phase of testing, we work to correct the deficiency or vulnerability prior to its deployment.

b. Are there vulnerabilities Dominion's is aware of that have not been disclosed to either its customers or the EAC?

Please see previous answer.

c. Please provide a list of discovered vulnerabilities, known failures, and malfunctions from the 2016 election until today that have been mitigated and how they were addressed by Dominion. Please also provide the number of discovered vulnerabilities, known failures, and malfunctions that have not been mitigated.

Given the volume of information this request entails, please contact the EAC for all product notices that our company and other manufacturers have submitted to the federal government in this regard.

18. Election critical infrastructure includes more than the machines upon which voters cast and count ballots. It includes voter registration databases, election night reporting system, and electronic poll books, for example. While voting systems can be tested and certified by the EAC, these other technologies are not reviewed and certified by the EAC. For Dominion's election products that are not voting systems, including those it manufactures and those that it sells or markets as companion products to its voting machines, how is Dominion ensuring that these products are safe, secure, and up-to-date and utilize current security best practices? How does Dominion check to ensure that its security best practices are effectively warding off attacks?

Dominion does not produce or sell any products that are not voting systems.

19. What voting machines does Dominion sell that currently have network capabilities (e.g. WiFi capabilities or Ethernet Ports) installed or as an optional add-on? Please provide the names of the machines and the type of network capabilities.

The ImageCast Precinct and the ImageCast Evolution can be paired with external modems.

20. Is it possible for states to purchase those devices without the network capabilities?

Yes.

21. What steps does Dominion take to secure its voting systems from the risks associated with a network connection?

Dominion voting systems are designed and certified to be closed, embedded systems when it comes to tabulator and election management functions. A very small number of jurisdictions (approximately 1% of our customer base) per their certification standards and contracts, require the secure transmission of unofficial results data to a county location. These customers are advised to carefully review their system documentation, consult with trusted security/IT providers and follow recommended best practices for secure system use, including:

- Disabling connectivity when not in use.
- Maintaining a hardened configuration for their voting system EMS installation.
- Maintaining access controls so that only authorized users can access the system.
- Monitoring all access and use.
- Maintaining strong password controls and other security measures, as recommended in product documentation.

22. If Dominion does sell machines with network capabilities installed or as an optional add-on, given the risks of network capabilities, why does Dominion continue to sell machines with this capability? What does Dominion think is its responsibility to notify the customers about the risks of having network capability?

Please see previous answer.

23. Despite the fact that in 2015 the EAC updated the Voluntary Voting System Guidelines (VVSG) by issuing VVSG 1.1, all of the voting systems that Dominion currently sells are certified to a fifteen-year-old standard, the VVSG 1.0. Why does Dominion choose to certify its voting systems to VVSG 1.0 rather than VVSG 1.1?

Meeting the latest standard is always important to us and our customers. Dominion has submitted systems for state certification based on the federal Voluntary Voting Systems Guidelines (VVSG) 1.1 framework. Our systems are currently able to meet this standard. The jurisdictions that we serve have been asking for modernized systems with enhanced security protections and robust capabilities for supporting post-election audits that go well beyond what is required in VVSG 1.1. Dominion is already shifting its development strategy with compliance against VVSG 2.0 in mind.

24. When Dominion sells add-on components to its EAC-certified systems that are not EAC-certified, what steps does it take to ensure its customers know those components are not EAC-certified? Does Dominion clarify this on its marketing materials? If not, why not?

Dominion works with every state and local customer to certify our systems, and this equipment is the only thing we can sell by law.[5] The company does not sell any class of equipment under an "add on"-type provision.

25. Once the VVSG 2.0 is in place, how long will it take Dominion to design and develop systems that meet those standards? Is it possible for Dominion to take steps now to prepare for the VVSG 2.0 to minimize the time lag?

Please refer to answer for Question 23.

26. What adversarial testing does Dominion perform on its voting systems? Please provide details and examples, including a list of the versions of the voting systems Dominion is currently selling that have gone through third-party adversarial testing.

As noted in an April 2019 response to the Committee, "We recognize that a proactive approach to discovering and remediating misconfigurations and vulnerabilities in voting systems is critical to reducing risk in the current threat environment. It is a driving factor behind our joint industry effort to create a Coordinated Vulnerability Disclosure Program via the IT-ISAC's Special Interest Group for Election Industry (EI-SIG). Additionally, as the only group of federally-regulated providers in the elections industry, voting systems manufacturers have both voluntary and compulsory testing performed on every system in use as part of mandatory federal and state certification processes. A number of factors determine whether a red team engagement is conducted as part of this testing, including customer demands, legal requirements and organizational system/process validation. Generally, penetration testing is used to identify and remediate vulnerabilities in products before they are certified for use. However, both federal and state election authorities can re-examine systems as needed."

"Adversarial testing can be performed by third-party providers, federally-accredited Voting System Test Laboratories (VSTLs) and partners (currently, two labs – SLI and Pro V&V) are independently certified by the EAC for this purpose) or CISA, via a partnership agreement with Idaho National Laboratory (INL). All of our companies have either had systems undergo free testing by CISA at INL, or we are discussing this voluntary offering as it relates to our current third-party testing schemes."

27. Without providing details about specific vulnerabilities in Dominion's system, what can Dominion share about what it has learned from adversarial testing?

[5] See National Conference of State Legislatures, *Testing and Certification of Voting Systems*, (August 6, 2018), https://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx.

Our team's knowledge of targets and strategies has evolved with our internal and external testing capabilities, particularly as new test cases and potential attack vectors are incorporated into the process.

28. In addition to the adversarial testing Dominion has performed on its systems, there are independent election security researchers that test its voting systems. In the Coordinated Vulnerability Disclosure Program white paper, Dominion and other vendors in the industry indicated a desire to "vet" researchers.[6]

    a. Some have said the industry's desire to place limitations on who can test its systems calls into question its commitment to truly open-ended public vulnerability testing. How does Dominion respond?

    Dominion has been consistent in our company's position that all testing must be conducted in a good-faith, professional and scientific manner, which aims to enhance public confidence in election outcomes. This is precisely why we work with third-party providers and independent Voting Systems Test Labs and federal, state and local election authorities to certify and publicly test all fielded systems for use. It is also why we are committed to working with other industry manufacturers to establish a CVDP for voting systems via the IT-ISAC, an effort which also includes some of the top white hat security researchers in the U.S.

    b. Has Dominion ever taken steps, such as threatening legal action, to try to prevent independent researchers from testing or gaining access to its products? If so, please provide details and explain why Dominion wants to prevent this testing.

    No, there are no instances where our company has sought criminal or civil penalties against an independent researcher in the wake of foreign attempts to interfere with the 2016 presidential election. We are now actively engaging and collaborating with more white hat hackers and independent researchers than ever before. Dominion adheres to the legal rights and protections established for good faith research specified in Digital Millennium Copyright Act (DMCA) Section 1201 exemptions, as well as federal and state criminal law.

    c. Is it Dominion's position that the modification, execution, possession, or transfer of its elections systems software by an individual without its consent using otherwise lawfully possessed or owned election systems hardware is a copyright infringement?

    This question requires a legal determination that we have not had occasion to consider. Any potential legal infringements or violations would be handled on a case-by-case basis, in which the applicable laws would be applied to pertinent facts.

29. What percentage of Dominion's revenue in fiscal years 2019, 2018, and 2017 did it invest in research and development? Please provide the percentage by year.

[6] *Coordinated Vulnerability Disclosure Program White Paper*, IT-ISAC, page 3, https://docs.wixstatic.com/ugd/b8fa6c_112b6b0bdc764533816b57dfdb3481b9.pdf.

As noted to the Committee in a number of prior communications, the range for those years has been eleven to twenty-five percent of gross profits to development, testing and certification efforts. Our founding principles include working collaboratively with all election stakeholders to maximize R&D development and deliver continual product innovation.

30. Taxpayer dollars are used to purchase Dominion's voting machines. It is important for taxpayers to know how the investment in research and development compares with the compensation of Dominion's executives. How much money in fiscal years 2019, 2018, and 2017 went to compensating senior management? What percentage of Dominion's revenue did that constitute?

Dominion is acutely aware of how much our company and its financial integrity matter to our customers and the taxpaying public. We are a privately-held company that is financially well-managed and run with the highest standards of integrity. As noted in his testimony before the Committee in January, Mr. Poulos is co-founder of the business and continues to manage the company as CEO. As discussed in his January 9th testimony before the Committee, Dominion reinvests eleven to twenty-five percent of its gross profits to development, testing and certification efforts annually.

31. During the hearing, Mr. Poulos confirmed that Dominion has private equity investors. What role does Dominion's private equity investors play in the direction setting of Dominion's policies and procedures?

Dominion's Board of Directors provides general guidance over company policies, but they are not directly involved in company administration or procedures.

32. Mr. Poulos testified that Dominion "had a policy that all employees were not able to make any campaign contributions."

    a. Please provide the Dominion policy governing campaign spending and/or campaign contributions.

    We appreciate the question and the opportunity to clarify our answer. Even where allowed by state laws and regulations, Dominion refrains from making any contributions to individual political candidates and political parties. Regarding company employees, many state laws prohibit employers from restricting employees to engage in political activities.[7] Therefore, it would be unlawful for Dominion to impose restrictions on employee political activity outside the workplace.

    b. Mr. Poulos testified that Dominion "had" a policy. Is the policy still in effect?

    See previous answer.

[7] For example, Colorado Revised Statues §8-2-108 states that it is "Unlawful for employer to prevent employees participating in politics. It is unlawful for any corporation, company, partnership, association, individual, or any employer of labor, or for any agent thereof to make, adopt, or enforce any rule, regulation, or policy forbidding or preventing any of his employees from engaging or participating in politics..."

c. What are the policy's effective dates, and is it still in effect?

See answer to 32a.

d. To whom does the policy apply?

See answer to 32a.

e. Does the policy cover corporate contributions?

See answer to 32a.

f. Does the policy cover employee contributions?

See answer to 32a.

g. Does the policy cover those with whom Dominion contracts?

The policy explained in the answer to 32A is not applicable to any vendors.

h. Does the policy apply to lobbyists at the federal, state, and/or local levels who do work on behalf of Dominion?

See answer to 32g.

i. What policies, if any, does Dominion have governing contributions to organizations organized under 26 U.S.C. § 527 (a "527 group")? Has Dominion made any contributions to a 527 group? If so, please provide the dates, recipients, and amounts.

See answer to 32a.

j. What policies, if any, does Dominion have governing contributions to nonprofit organizations, including membership associations? Has Dominion made any contributions to such organizations? If so, please provide the dates, recipients, and amounts since 2010 and the purpose of the contributions.

Dominion is proud to support non-profits and charitable giving organizations that align with our company's mission. For example, the company matched all employee contributions for donations to Puerto Rico after the island was devasted by Hurricane Maria. We also contribute to non-profit efforts to support elections in developing countries.

k. How are these policies enforced?

Our reporting and compliance obligations under law are the same as those of any other company doing business with state and local governments. Dominion has always been in good standing with such legal requirements, as previously affirmed to this Committee in our communications.

33. Concerning Dominion's lobbying and marketing practices and policies:

a. What percentage of Dominion's budget was spent on lobbying in fiscal years 2019, 2018, and 2017? How much money did that constitute in dollar figures? How are those funds spent?

As a U.S.-owned company in good standing, Dominion employs no in-house lobbyists. All external legal contracts comply with federal and state disclosure requirements under law. Specific to Congress, the company has focused on educating lawmakers about the voting systems industry and how our products are designed, tested, certified and secured. The company has received an unprecedented number of congressional inquiries and requests for briefings from the company in the past three years. Dominion spends approximately 0.5% of budget on lobbying activities. All contract amounts are available in regular public disclosure reports, as required by law.

b. What percentage of Dominion's budget was spent on marketing in fiscal years 2019, 2018, and 2017? How much money did that constitute in dollar figures? How are those funds spent?

Dominion spends approximately 0.1% of budget on marketing.

c. Please provide a list of jurisdictions in which Dominion has registered lobbyists.

Dominion currently retains such representation in California, the District of Columbia, Georgia, Hawaii, Illinois, Louisiana, Nevada, New Jersey, New York and Pennsylvania.

34. According to a June 2018 McClatchy article, ES&S maintained at the time a "Board of Advisors" comprised of election officials that are responsible for negotiating and awarding voting system contracts.[8]

a. Does Dominion now or has it ever maintained a similar customer board?

No.

b. If so, please provide a list of all past and present members.

N/A

c. Does Dominion pay for travel and entertainment for this board to attend meetings about Dominion products? Please provide details.

N/A

35. In response to Chairperson Lofgren's question: "Do all of your election systems currently in use prevent unauthorized code or altered operating systems from running on them in this way?" Mr. Poulos responded: "All of our Dominion products that are certified are the same. The exception that

[8] Greg Gordon, et al. "Voting machine vendor treated election officials to trips to Vegas, elsewhere," *McClatchy* (June 21, 2018) https://www.mcclatchydc.com/latest-news/article213558729.html.

I will point out to the Committee is we do support some legacy systems that are still in use that were designed in the remaining cases over 20 years ago that do not have this capability." However, the 2019 DEFCON Voting Village Report indicates that Dominion's Imagecast Precinct allowed booting of arbitrary, unsigned operating systems from a USB or CF card (which would also allow unsigned code to run), and it allowed unsigned configuration files to change vote scanning configurations.

a. The Imagecast Precinct is Dominion's newest optical scan tabulator. Given this example of Dominion's newest optical scanner lacking protection against the running of unsigned code or altered operating systems, would Mr. Poulos like to clarify his statement to the Committee?

Please note that DEFCON acquires equipment from undisclosed sources, which makes it challenging to verify what is actually being analyzed. Based on our review of the September 2019 findings from the DEFCON Voting Village report, the ImageCast Precinct unit that was acquired appears to be an early prototype that was never certified for use in any jurisdiction.

As Mr. Poulos mentioned in his testimony to the Committee, Dominion had an existing agreement to provide certified systems for DEF CON last summer, but it was rescinded at the last-minute by Voting Village organizers. While we were unable to renegotiate the terms for that effort, senior company officials were able to attend DEF CON and interact with researchers, ethical hackers and election officials while showcasing our latest equipment. Dominion remains committed to working on collaborations with the researcher and security communities.

b. Can Dominion please provide to the Committee a whitepaper or more technical description of how exactly its unsigned code protection works? Disclosure of such details is common practice among computer and smartphone vendors, who have both publicly disclosed technical details of how their secure boot and code signing protections work.

Please see answer to Question 26.

MINORITY QUESTIONS FOR THE RECORD

1. Could you describe in detail how some of your machines are able to assist voters with disabilities?

According to the U.S. Election Assistance Commission, more than 35 million Americans with disabilities are eligible to vote in the U.S., accounting "for a broad range of disabilities, including mobility, communicative, physical and cognitive impairments." Dominion voting systems meet or exceed all federal standards for assisting voters with disabilities, including wheelchair access, audio voting (with and without visual display), two input switches (i.e. sip and puff), vote from home capabilities (i.e. UOCAVA voting), and more.[9] All modules used to assist voters with disabilities have multilingual capabilities, depending on

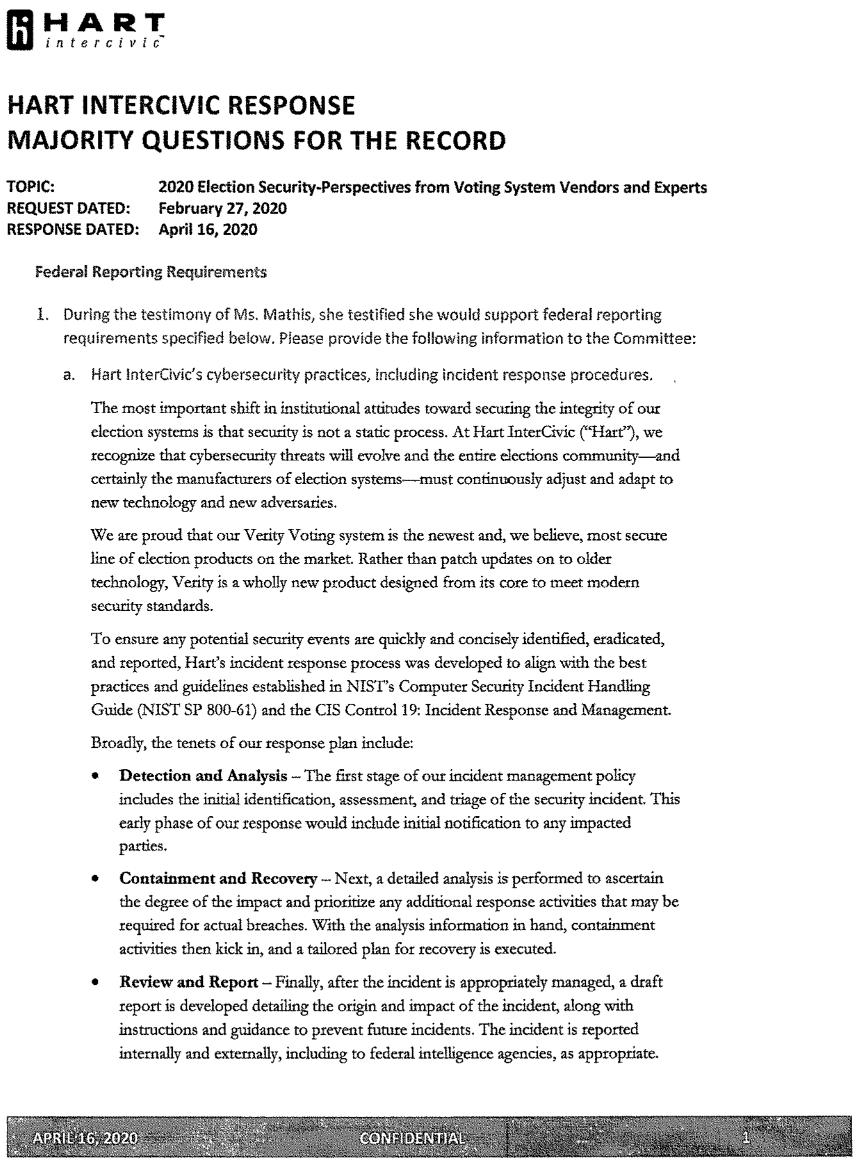
[9] See EAC Voluntary Voting Systems Guidelines, https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines.

the jurisdiction's language requirements. The general goals with any type of accessible voting system are to ensure that voters can cast their ballot privately and independently, with the same dignified experience as any other voter. Dominion Democracy Suite systems also mark ballots in such a way as to make it impossible to distinguish between the cast ballots of disabled and able-bodied voters.

2. In your testimony you mention Congress needs to remove barriers which exist to modernize election infrastructure. What are the barriers that exist which should be removed?

As noted in hearing testimony as well as briefings, we believe that Congress can play a useful role in helping election officials deal with the following challenges:

1) Dedicated funding for state and local election officials
2) Streamlined certification options for de minimis changes to voting systems, such as patching and updating, as needed
3) Required testing and certification standards for all elections technology prior to deployment and use



HART intercivic

HART INTERCIVIC RESPONSE
MAJORITY QUESTIONS FOR THE RECORD

TOPIC: **2020 Election Security-Perspectives from Voting System Vendors and Experts**
REQUEST DATED: **February 27, 2020**
RESPONSE DATED: **April 16, 2020**

Federal Reporting Requirements

1. During the testimony of Ms. Mathis, she testified she would support federal reporting requirements specified below. Please provide the following information to the Committee:

   a. Hart InterCivic's cybersecurity practices, including incident response procedures.

   The most important shift in institutional attitudes toward securing the integrity of our election systems is that security is not a static process. At Hart InterCivic ("Hart"), we recognize that cybersecurity threats will evolve and the entire elections community—and certainly the manufacturers of election systems—must continuously adjust and adapt to new technology and new adversaries.

   We are proud that our Verity Voting system is the newest and, we believe, most secure line of election products on the market. Rather than patch updates on to older technology, Verity is a wholly new product designed from its core to meet modern security standards.

   To ensure any potential security events are quickly and concisely identified, eradicated, and reported, Hart's incident response process was developed to align with the best practices and guidelines established in NIST's Computer Security Incident Handling Guide (NIST SP 800-61) and the CIS Control 19: Incident Response and Management.

   Broadly, the tenets of our response plan include:

   - **Detection and Analysis** – The first stage of our incident management policy includes the initial identification, assessment, and triage of the security incident. This early phase of our response would include initial notification to any impacted parties.
   - **Containment and Recovery** – Next, a detailed analysis is performed to ascertain the degree of the impact and prioritize any additional response activities that may be required for actual breaches. With the analysis information in hand, containment activities then kick in, and a tailored plan for recovery is executed.
   - **Review and Report** – Finally, after the incident is appropriately managed, a draft report is developed detailing the origin and impact of the incident, along with instructions and guidance to prevent future incidents. The incident is reported internally and externally, including to federal intelligence agencies, as appropriate.

b. Any cyberattacks Hart InterCivic has experienced. This should include any phishing attempts Hart InterCivic has detected.

We have never experienced an incident that we have identified as a cyberattack on any Hart owned or operated system. Should we ever identify malicious or inauthentic activity against our systems, our Incident Response Plan requires notification to the Dept. of Homeland Security (DHS) and the IT-ISAC (EI-SIG) [Election Industry-Special Interest Group].

Like all public offices, government facilities, and private companies, we receive generic spam and phishing emails daily. Any potentially threatening emails are routinely identified and quarantined through our spam filter and our staff is trained on how to identify and mitigate malicious emails.

We have taken this responsibility a step further and assisted local election officials to report phishing emails received by their offices. In the fall of 2019, we were contacted by one of our customers regarding a likely phishing email that purported to be from Hart. We immediately assisted the official to determine the email was not from us and should therefore be reported. In coordination with the election official, we captured a screen shot of the email and reported it directly to DHS and the IT-ISAC (EI-SIG) so that the offending email content and domain address could be investigated and shared across the industry.

c. Personnel policies and procedures, including whether background checks and other procedures are in place to safeguard against inside attacks and how Hart InterCivic assesses current employees on an ongoing basis for security risks. Please specify the policies and procedures.

As a company that designs and builds the devices on which our American democracy is managed, we take all threats – whether external or internal – extremely seriously. Therefore, all new employees are required to submit to a background check, a drug screen, and a motor vehicle check. Additionally, on an annual basis, Hart rescreens our existing staff through new background and motor vehicle checks.

d. Details of corporate ownership and foreign investment. Please submit a list of all individuals and entities with a five percent or more ownership or control interest in Hart InterCivic, including private equity investors, and indicate the percentage of ownership or controlling interest. Please also provide a list of all investment by foreign entities and individuals in Hart InterCivic.

Hart InterCivic is owned by a private equity fund managed by H.I.G. Capital, LLC, a leading U.S. private investment firm based in Miami, Florida. The controlling interest in H.I.G. Capital, LLC is held exclusively by U.S. citizens. The fund does have passive investors located outside of the U.S., although none of those investors own a greater than five percent investment. Beyond the H.I.G majority ownership, Hart has one additional investor with a stake in the company greater than five percent – an individual American citizen in Austin, Texas. No other individual, corporation, organization, or limited partner owns a greater than five percent share of the business.

e. Details on Hart InterCivic's supply chain, including where parts, software patches, and installations come from; how are they transported; and how they are kept secure.

   See our responses to Questions #3-8.

Other Reporting Requirements

2. In addition to reporting the information above discussed during the hearing, please provide the following information to the Committee. This is all information that Hart InterCivic is required to provide to at least one of the states in which its machines are certified:

   a. Management and staff organization; number of full-time employees by category; and number of part-time employees by category.

   b. Financial history of the business, including a financial statement for the past three fiscal years.

   c. History and description of the business, including year established; products and services offered; states with machines Hart InterCivic's manufactures or services; branch offices and subsidiary and/or parent companies.

   d. Audited report of the business' fiscal year 2019.

Hart is a privately-owned company based in Austin, Texas, where we have conducted business for over 100 years. Originally a paper printing company, Hart first entered the voting system market just after the 2000 Presidential Election. We are run and managed locally in Austin by a seasoned executive team with deep knowledge of the elections industry and a combined 45 years of experience in the field.

Currently, we supply the voting systems that state and local officials use to run their elections in 19 states. We have grown our customer base organically, one customer at a time, with no acquisitions of other voting system companies. Our substantial customer growth and consistent high customer satisfaction scores are indicative of the quality of our products and service and the financial health of our company. This year, we will support elections in California, Hawaii, Idaho, Illinois, Indiana, Kentucky, Michigan, Minnesota, Mississippi, Missouri, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, Tennessee, Texas, Virginia, Washington, as well as in several Native American nations.

We are working closely with every one of our customers to ensure they have the equipment, support, and knowledge they need to provide accessible and secure elections, especially given the COVID-19 pandemic that is rapidly altering election dates and voting methods (e.g., nearly every election jurisdiction in the nation is considering how they may handle a significant increase in vote-by-mail). In addition to supplying our customers with reliable and secure voting devices, we also regularly provide webinars, newsletters, white papers, and user groups in order to keep our customers well-informed of the latest best practices and trends in election administration and security. Last month, for example, we held multiple webinars for our customers on best practices and key considerations for expanding vote-by-mail programs.

Our commitment to service is reflected in our customer satisfaction rates. Over the past eight years, more than 90 percent of our customers have rated our service and support as "excellent" or "above average." Additionally, election officials that have moved to Hart from another vendor over the past three years – representing more than a third of our current customer base – made that decision in order to take advantage of the technology innovation, security features, and service that only Hart provides.

As the Committee is aware, though many states allow for limited disclosure of information collected through their state certification processes, each state has specific rules and procedures for accessing that information. Without authorization from the state certification authorities, we risk violating state regulations by providing protected information in a public document. The Committee may check with the individual states for access to the requested information. All information on federally certified election systems can be accessed publicly through the Election Assistance Commission (EAC): https://www.eac.gov/voting-equipment/voting-system-reports-collection/.

Supply Chains

3. During the January 9, 2020, hearing, Ms. Mathis could not provide the Committee with the precise percentage of components from China on the spot. For all the questions below, please also provide specifics on the relevant components by describing them; whether they are inert or programmed or programmable; and the machines for which those components are used.

   Hart places the highest importance on supply chain security and proactively takes proven, best-practice measures to ensure the integrity of every vote cast on our devices:

   - Like all U.S.-registered voting systems manufacturers, we provide extensive product sourcing information to the EAC and state election offices as part of the certification and testing process. We also work closely with U.S. election officials and other government partners to test and certify our systems for security, accuracy, and reliability in each and every election.
   - Voting systems are routinely subjected to rigorous review, analysis, testing and certification by election authorities at the federal, state, and local levels. Once the system is certified, any changes – including to supply chains and components – prompts a new round of review and testing by government authorities. This process helps to ensure that potential product vulnerabilities are discovered and addressed on a timely basis.

- Voting system manufacturers work to define reasonable levels of security and associated controls for our supply chains, including requiring sub-contractors and vendors to meet or exceed standards as part of the terms and conditions of our established business agreements. We also employ tools and resources to technically and operationally mitigate risk across the lifecycle of products, from design through disposal.

The practice of assessing risk based solely, or even primarily, on the geography of a supplier's corporate locations can inadvertently lead to a false sense of the security around the components. Supply chain threats exist regardless of where a company is headquartered or where its products are manufactured and assembled.

A better approach is to treat every component in a supply chain, regardless of origin, with caution and healthy suspicion. At Hart, we conduct regular assessments and audits of every component that goes into Verity, even those that are inert, on their point of origin, including safe-handling protocols, tracking of inventory, secure container locks and tags for products in transit, and monitoring of both external and internal risks to technology and data.

Unlike other companies in our industry, we are able to maintain tight control and management of our supply chains because every single Verity device is manufactured locally in Austin, Texas. Our commitment to the integrity and security of our products remains our top priority and we are constantly evaluating and adjusting our global supply chains in real time.

The responses provided throughout the rest of Question #3 are related to the electronic components within Verity Voting devices.

a. Please provide the percentage of the components in Hart InterCivic's supply chain that come from China.

   Less than one percent of the electronic components within Hart's voting devices are programmed or programmable components that originate in China.

b. Please also provide the percentage of components in Hart InterCivic's supply chain that come from foreign countries other than China. Please provide the country and percentages by country.

   Approximately one percent of the electronic components within Hart's voting devices are programmed or programmable components that come from countries other than China or the United States. *Of that one percent*, the countries include Taiwan and Thailand with percentages between 20 and 40 percent each; Singapore and Malaysia with between nine and 15 percent each; and Germany and Vietnam at five percent each.

c. Please provide the percentage of components come from China-based companies.

   There are no known electronic programmed or programmable components within Hart's voting devices that come from companies that are headquartered in China.

d. Please provide the percentage of suppliers in Hart InterCivic's supply chain that have locations in either China or Russia.

Less than one percent of the electronic components within Hart's voting devices are programmed or programmable components that come from companies with manufacturing sites in China. None of our suppliers, to the best of our knowledge, have manufacturing sites in Russia.

4. In addition to concerns about the components in Hart InterCivic's supply chain, the Committee requests more information on Hart InterCivic's software development.

a. Where is Hart InterCivic's firmware and software developed? If it is developed in multiple locations, please specify those locations.

Hart's firmware and software are developed in Austin, Texas.

b. Where is it installed?

Hart's firmware and software are installed in Austin, Texas.

c. How does Hart InterCivic protect it from remote access and tampering from outsiders? Please provide specifics.

As a critical aspect of our business, we have ardent security protections in place to protect our software development process. We apply a wholistic Defense in Depth approach to security (further described in our response to Question #32), building layered, redundant security checks around our systems that account for the security posture of the people, process, procedures, and technology.

The safeguards we have put in place to protect sensitive data in storage and transfer include:

- All Hart groups that handle sensitive data maintain air gapped networks, thereby reducing their attack surface.
- Any sensitive data that is transferred physically is moved on secure, encrypted USB memory devices equipped with virus protection following strict chain-of-custody protocols for tracking purposes.
- Data transfer occurs over a secure VPN.
- Hart networks are protected through multiple redundant firewalls that are supported and monitored by our security provider – one of the leading cyber defense firms in the nation.
- We apply content URL filtering of web traffic and mail filtering for spam and malware.
- Hart's core networking switches are monitored and managed 24/7 by our security provider.

- Access to any Hart file server is available only through a VPN connection and requires a domain account and Two-Factor Authentication.
- All Hart networks have undergone vulnerability assessments through our security provider.
- Stringent user security practices are deployed across our system, including: Two-Factor Authentication, password protocols, regular security notifications, and routine backups of data.
- All Hart user accounts are required to be active directory domain accounts, and permission to files and folders are set for least privilege.
- In addition to all of our technological defenses, all Hart employees are screened prior to hiring and rescreened on a routine basis.

5. For components that are manufactured in other countries, like China and Russia, is it possible for you to find different manufacturers that are in the United States or in countries that have not been accused of committing cyberattacks against the United States? If not, why not? For example, is the component protected by a patent?

During the hearing, all three companies noted the industrywide use of a class of inert components – those that are neither programmed, nor programmable – that are not produced or available from United States sources. While some of those components originate in China, we do not source any part or component from Russia.

As mentioned above in our response to Question #3, Hart's policy is to treat each component in our supply chain, regardless of origin, with caution and healthy suspicion. We regularly assess and audit every component in our supply chain – including inert components – on their points of origination, including safe-handling protocols, tracking of inventory, secure container locks and tags for products in transit, and monitoring of both external and internal risks to technology and data.

We are constantly exploring both the domestic and global markets to ensure our Verity Voting system is manufactured with the best components from trusted sources at the lowest price. As discussed during the hearing, we welcome – and have requested – additional guidance and best practices on supply chain security from DHS.

6. In Hart InterCivic's response to the Committee's September 19, 2019 letter asking questions about how Hart InterCivic protected the security of its supply chain, Hart InterCivic provided some best practices which it follows. How specifically does Hart InterCivic know that its best practices are working – if they are – and that its supply chain is secure? What checks does Hart InterCivic have in place?

Ensuring that a supply chain is fully mapped, controlled, and regularly monitored, from design through final delivery of a device, is a necessity across all private industry in the United States, but is particularly imperative to companies that supply sectors of Critical Infrastructure.

At Hart, we recognize that a sustainable supply chain, coupled with stringent security controls, is not a luxury – it is critical for our products and our customers, and therefore, our own financial stability.

The primary checks of our supply chain protection process include:

- We are in direct control of our supply chain – it is a closely managed element of our business.
- We partner with trusted suppliers with longstanding reputations for quality control.
- We require stringent security assurances and protocols in agreements with our manufacturing partners.
- Our Verity Voting system is manufactured in our hometown of Austin, Texas, giving us direct control and oversight of the entire Verity build process.
- From design to assembly, the Verity build is governed by a secure engineering change order control process.
- Verity's manufacturing facility is certified to both the ISO-9001 and International Traffic in Arms Regulations (ITAR) standards.
- We apply the Customs Trade Partnership Against Terrorism (CTPAT) program across our supply chain.
- To prevent counterfeit parts from being installed in our devices, we strictly follow the IPC 610 Class II standard for screening components prior to assembly.
- We employ strict authorization processes with detailed step-by-step procedures for logging, securing, and tracking the chain of custody of our products according to individualized serial numbers for each unit.
- When shipping a product to an election official, we follow state-specific mandated policies for handling new or returned equipment per the state's guidelines. When providing election devices or systems in states without prescribed policies, we employ industry best practices.
- Our supply chain is regularly reviewed and audited for new risks, and our policies are continuously updated to address new vulnerabilities.

7. Interos wrote on page five of its report Election Technology & the Global Supply Chain that it notified the manufacturer of the machine that was the subject of the report.[1] It states that "Interos recognizes the extreme sensitivity of election security matters and has contacted the affected company involved." Has Hart InterCivic company been notified by Interos that it is the vendor that manufactured the machine discussed in the report?

We have never been notified by Interos that we are the company discussed in the report.

[1] *Election Technology & the Global Supply Chain*, Interos, (Dec. 16, 2019), page 5, https://cdn2.hubspot.net/hubfs/5812029/Interos%20-%20Election%20Security%20Paper.pdf.

8. What steps does Hart InterCivic take, if any, to ensure that subcontractors and manufacturers producing its components overseas are not subject to influence from a foreign government?

   At Hart, we know that supply chain security is paramount to the integrity of election infrastructure and may have a direct impact on voter confidence and participation in our democracy. Though we do not run elections, we are acutely aware of our role in securing America's election process and take that charge seriously.

   To ensure we meet this responsibility, we apply robust security procedures and regular audits to our supply chain to ensure the quality and integrity of every component that goes into the Verity Voting system, regardless of the component's point of origin. See our response to Question #6 for a comprehensive list of the security checks in place to safeguard our supply chain.

   Two programs that we have deployed within our supply chain that directly protect against potential influence from foreign actors are the Customs Trade Partnership Against Terrorism (CTPAT) and the International Trade and Arms Regulations (ITAR). These two programs are specifically focused on enhancing the security posture of private industry supply chains. By voluntarily requiring CTPAT and ITAR within our supply chain, we gain greater assurances of the integrity of every electronic component that goes into our devices.

Ballot Marking Devices

9. Studies on the use of ballot marking devices show that voters check their ballots at very low rates and alert election officials to errors at an even lower rate. Is Hart InterCivic working to design ballot marking devices or to identify other technical solutions that improve the rate of voter verification of their printed ballots to ensure that there is a reliable voter-verified paper trail from its ballot marking devices that can be audited with confidence?

   Hart is one of the only election system manufacturers in the country with an EAC-certified ballot marking device that does not place vote selections in a barcode or QR code, making it possible for voters to personally verify their choices on their ballots.

   Our ballot marking device, Verity Duo, produces a printed ballot with a clear, legible summary of the voter's choices, including the name of the contest, the full name of the selected candidate, and the candidate's party. The ballot produced by Verity Duo is processed and tallied using Optical Character Recognition (OCR), which means the scanner reads the same printed words that the voter verified.

   In addition to implementing good design principles into the voting devices themselves, process plays a key role in ensuring that voters verify their ballot selections. The same academic study on which this question is premised also found that review and detection of ballot errors by voters rose dramatically when poll workers simply reminded the voters to double-check their ballots prior to submission. To that end, we intentionally designed Verity to make such voter education efforts easy for election administrators.

Verity Duo allows officials to customize the final "closing" screen voters see before submitting their ballots, and we actively encourage all our customers to include language on the screen that reminds voters to verify their selections before casting their ballots.

10. During the testimony of Ms. Mathis, she testified that Hart InterCivic does not sell equipment that tabulates votes based on a barcode or QR code.

    a. Please specify how Hart InterCivic's ballot marking devices tabulate votes.

    Verity Duo is one of the only federally certified ballot marking devices on the market that utilizes Optical Character Recognition. Voter selections are never contained in bar codes or QR codes on the Verity Voting system.

    b. What steps does Hart InterCivic take to ensure that voters can be confident that their choices will be counted accurately?

    All versions of Verity are tested and confirmed to comply with accuracy requirements defined by the VVSG 1.0 volume I, section 4.1.1 standard. These requirements are defined in the standard as the ability to capture, record, store, consolidate, and report specific selections and the absence of selections made by the voter for every ballot position without error.

    These requirements are applicable to all elements in the Verity system that detect or record vote selection data including our paper-based and electronic devices, central scanners, and tabulation workstations.

    The EAC's VVSG certification process requires accuracy testing while the voting system is under environmental stress, with accuracy being measured during power and temperature fluctuations designed to mimic real-world polling place conditions. All Verity devices on the market have passed through this rigorous testing process.

    Additionally, we actively partner with our customers to assist them in performing election device testing and auditing throughout the election process, providing further assurances to voters that their ballot was recorded as cast. This includes logic and accuracy testing both prior to and after an election, as well as rigorous post-election audits, including Risk-Limiting Audits.

Guidance on Identifying and Mitigating Security Risks

11. As we discussed during the hearing, the Consumer Product Safety Commission advises manufacturers of consumer products to "identify all reasonably foreseeable hazards associated with" their products and include safety warnings and steps to reduce risk in the user guides. There are similar requirements for motor vehicles and warnings in owner's manuals. During the hearing, Ms. Mathis testified she would support a requirement for voting system vendors to provide guidance to customers identifying security risks associated with use of Hart InterCivic's equipment and recommendations to mitigate those risks.

a. Does Hart InterCivic currently include such guidance for election officials buying its products?

Yes. Hart devices are designed to mitigate hazardous risks. Every device we manufacture is delivered to our customers with a set of comprehensive product user manuals that provide detailed guidance for the safe and secure operation of the device. We then reinforce that guidance through requisite, and repeated, training sessions with our customers.

b. If yes, please detail what is included.

Most relevant to issues of concern for the Consumer Product Safety Commission, those instructions include topics that cover:

- How to request support
- Equipment specifications
- Device storage and transport
- Acceptance testing
- Functionality testing, including:
    - Touchscreen
    - Device report printer
    - Controller
    - Ballot printer
    - Scanner
    - Battery backup
- Device setup
- Power supply
- Checking/replacing battery
- Starting/restarting a device
- Checking headphones and audio settings
- Testing handicap accessible input devices
- Cleaning the scanner
- Preventative Maintenance
    - Frequency/schedule
    - Cleaning touchscreens
    - Calibrating touchscreens

    - Cleaning scanners
    - Calibrating scanners (speed/contrast)
    - Scanner multi-feed calibration
    - Paper sensor calibration
    - Replacing tablet CMOS batteries
- Device settings
- Security recommendations
    - For polling place devices
    - For central processing devices

c. If no, isn't it reasonably foreseeable that an election official might need that guidance or warning, particularly in the current threat environment? Why does Hart InterCivic choose not to provide such guidance? Does Hart InterCivic have any plans to do so in the future?

N/A.

d. Does Hart InterCivic provide any instructions concerning audits? Does Hart InterCivic recommend risk limiting audits?

Yes. We provide our customers with detailed instructions and guidance on how to perform audits on our devices.

Effective audit practices, such as risk-limiting audits (RLA), are an essential component to the integrity of every eligible American's vote. Audits not only increase the likelihood that any malicious tampering or malfunctioning machine in an election is detected and corrected, they provide the public with needed assurance that the outcome of an election contest was accurately determined and reported. Hart unequivocally supports state efforts to strengthen election auditing procedures.

To that end, we have partnered directly with leading advocacy organizations that have developed RLA tools for local election officials and have participated in RLA-focused trainings sponsored by state and county election officials.

e. Given the security concerns around logic and accuracy auto-testing, and the failures that happened in Northampton County, PA in 2019,[2] does Hart InterCivic recommend manual logic and accuracy testing for every ballot style? How many of Hart InterCivic's machines have an auto testing feature?

[2] Tom Shortall, *No Confidence: Northampton County election board 'extremely disappointed' in machines it selected*, The Morning Call (Dec. 19, 2019), https://www.mcall.com/news/local/mc-nws--20191220-xrkqrrokfrgzlc3lglpn5nf5fe-story.html

Yes, we strongly encourage our customers to perform logic and accuracy testing both prior to and after each election across all ballot styles, in accordance with state regulations.

Unlike the events that occurred in Northampton County, Hart never allows automatic logic and accuracy testing on any of our voting devices. Automating the functionality of the testing would not only undermine the purpose of the testing itself but would likely introduce new security concerns.

f. What other election day support does Hart InterCivic provide to its customers? If this varies based on the contract, please provide specifics on the different contracts Hart InterCivic has and the support provided in each and the price difference between the levels.

Election Day support is a critical function of our relationship with our customers. Every one of our customers receives professional and timely support from our Customer Support Center every day of the calendar year. And for all major Election Days, we shift staff over to the Customer Support Center to ensure that any election officials who contact us receive an immediate response.

We also offer on-site support on Election Days. The rate for on-site support is built into the project management package of all our contracts and remains flat across the life of a customer's agreement, whether on an Election Day or just an average Tuesday. Jurisdictions then opt-in to on-site support as their needs dictate.

We are consistently rated with the best published service ratings in the elections industry, a track record of which we are exceptionally proud. All of our customers, regardless of their location or size, receive the same excellent services.

Cybersecurity Protections

12. During the hearing, Ms. Mathis said that Hart InterCivic currently employs a certified information systems security professional (CISSP), but not a chief information security officer (CISO).

a. What is that individual's title?

Principal Security Engineer, CISSP.

b. How long have they been on staff?

Nine years.

c. What authority do they have within the company?

As Hart's Principal Security Engineer and CISSP, this individual has a leadership role in setting the security posture throughout our company and our products. The individual's responsibilities cut across our entire business, including guiding the Verity build and certification process, as well as our incident response efforts on any cybersecurity event that could impact our products or our internal systems.

d. Does that person hold any other titles or responsibilities within the company?

No.

e. Why has Hart InterCivic chosen to hire a CISSP rather than a CISO?

As described during the hearing, we have formed a dedicated, cross-functional Security Team comprised of Hart's executive leadership, department heads, and essential staff members, such as our CISSP, alongside our CEO, Ms. Mathis, herself. The Team has ongoing strategies, communications, and tactical projects, along with recurring meetings to engage on all issues of cybersecurity affecting our company and our industry.

A team strategy allows us to effectively manage our cybersecurity defenses through regular engagement with the primary department leads across the company and makes security a priority for the entire team. Team members are assigned clearly defined roles, and the routine meetings provide a dedicated forum for the discussion and analysis of security issues, along with a means to hold team members accountable for the completion of tasks assigned during meetings.

To ensure that Hart's awareness and focus in the cyber security arena stays relevant and in consideration of all current known indicators, we also engage with outside experts and credentialed consultants to supplement our own efforts. In addition to regular interaction with DHS, the EAC, and the EI and IT-ISACs (as previously detailed during the hearing and in past inquiries from the Committee), we have also engaged directly with trusted experts in the field of cyber security. We have brought in, and will continue to bring in, security consultants and firms that are nationally recognized experts in the field of security management to assess our systems and corporate policies against relevant federal standards, such as the NIST Cyber Security Framework and CIS Controls, and make recommendations on where and how we could improve.

13. Does Hart InterCivic have technical staff with cybersecurity expertise involved in all stages of the product—the marketing, the design, the testing, the service, and support?

Yes. A core tenet at Hart is that security is a fundamental architectural and design requirement across all product development, quality, and regulatory requirements, along with all sales, marketing, service and support functions. We take security seriously and our team approach enforces this tenet cross-functionally within the business.

Both our Chief Technology Officer and Principal Security Engineer and CISSP play vital roles in ensuring continuity of security processes across all stages of our product development and support. Their oversight and impact throughout our company is both direct and cross-functional through their roles on the Hart Security Team, as described in our response to Question #12(e). Additionally, we manage our focus on security through a rigorous, structured, documented phase gate process in which regular security audits and threat assessments are conducted before progressing from one phase of the process to the next. This process is closely managed by Hart senior management and reviewed throughout the entirety of the phase gate process.

14. When Hart InterCivic, or someone Hart InterCivic contracts with, assists jurisdictions with programming services, how are those files delivered to the jurisdiction? What steps do you take to ensure the transfer and delivery of the programming files is secure? What steps do you take to secure the device the programming actually takes place on?

We follow security best practices and chain-of-custody protocols, as described throughout this QFR response, when transferring any files with election offices. For file transfer, some of the specific security procedures we have adopted include:

- Files are delivered to customers through a secure transfer protocol.
- Access to files is limited to known and logged-in users from known and logged-in administrators.
- Access is password protected and requires Two-Factor Authentication.
- We are notified any time a file is accessed.
- Files are deleted after they are accessed.

Any data transfer that involves the transmission of ballot layout or "programming files" occurs on certified equipment that is air gapped from all other Hart networks. The media that is used on these certified systems is always scanned prior to use and is verified to be either new or wiped from its previous use. Additionally, Hart never contracts with third parties to provide programming services to our customers – all work is performed by qualified Hart staff.

Voting System Vulnerabilities and Updates

15. The Election Assistance Commission (EAC) issued a Notice of Clarification on De Minimis Software Changes in November of 2019.

a. Has the EAC's Notice of Clarification on De Minimis Software Changes made the certification of security updates easier?

We are a very vocal supporter of the EAC's efforts to update and expand the process for De Minimis software and security updates. It is our belief that this modernization of the federal certification process will improve the integrity of the entire U.S. election system.

It has not yet been necessary for us to utilize the updated process, but we are optimistic that it will ease the process and improve the speed for the certification of De Minimis updates.

b. Has that Notice solved the issue with delays to the certification of security updates?

Though we have not yet utilized it, we believe the updated process for De Minimis changes will allow for more efficient, and therefore faster, certification of qualifying security and software updates.

c. How does Hart InterCivic ensure that states receive security updates for their voting systems?

We analyze any new security update as it is released to determine the impact on deployed systems and our systems that are currently in development. We then work simultaneously to move the update through federal and then state certification processes, while engaging directly with our customers to plan out the most feasible timeline and deployment strategy that works within their calendars and existing infrastructure.

d. On average, once an update is certified, how long does it take for a state to receive that security update?

Upon notification of EAC-certification, we are typically able to submit updates to state certification agencies within one week.

Once submitted to a state, timeframes for state agency approval vary widely across the country. Hart makes every effort to move through state certifications as quickly as the process allows, which can range from a matter of weeks to nearly a year.

e. How is the security update transmitted to the local election officials? What are the costs associated with getting a security update or patch?

Upon notification of EAC certification (all Verity Voting systems are federally certified, regardless of state requirements), two processes begin simultaneously: our Certification team will enter the update into the state's own certification process, while our Operations team begins to coordinate with all impacted local election offices. In full cooperation and coordination with the election officials, we develop a customized plan for the most feasible timeline for implementation, with specific consideration for any upcoming election dates on the calendar. Our intention is to be prepped and ready for deployment upon exit of the state certification process.

Since Hart never employs remote access into our Verity Voting devices, any update – whether related to security or otherwise – is installed by qualified Hart staff. And all general release security updates and patches are included as part of our customers' contracts as a part of license and support services Hart provides.

16. Your company regularly submits updated voting systems to the EAC for certification.

a. Once an updated system is certified, do jurisdictions have the opportunity to update their systems?

Yes. The process for assessing which jurisdictions require the update and the coordination with the jurisdiction for deployment is the same as that described in our response to Question #15.

b. How does this process work? For example, is a physical intervention needed?

Same process as described in our response to Question #15(e).

c. Is the process different if the update is certified by the EAC as a new system versus a modification?

At the federal level, the process to update new systems vs. modifications is not significantly different. However, depending on the jurisdiction, new systems often require more extensive state certification testing than that required for modifications.

d. For machines that run a version of Windows that has reached the end of its life, will Hart InterCivic provide updates to jurisdictions?

Yes, as described in our response to the Committee's inquiry to voting system manufacturers from July 24, 2019, we have a detailed plan for upgrading Verity's embedded operating system years prior to its anticipated end-of-life.

However, older legacy devices still in use by election officials present unique challenges. We will continue to provide support for all Hart voting devices as long as they are actively used by our customers, but many of those election officials will be better served by moving to newer election technology that is designed to address modern security and accessibility concerns.

We are upfront with our customers who still run elections on aging voting devices – their best path to secure the elections they oversee is through newer voting technology. Though we cannot make the decision for our customers, we offer frank and honest advice that moving to a more modern and secure platform is the strongest move to ensure the integrity of their citizens' vote.

e. If so, what will the process be for those updates and will Hart InterCivic be charging jurisdictions for those updates?

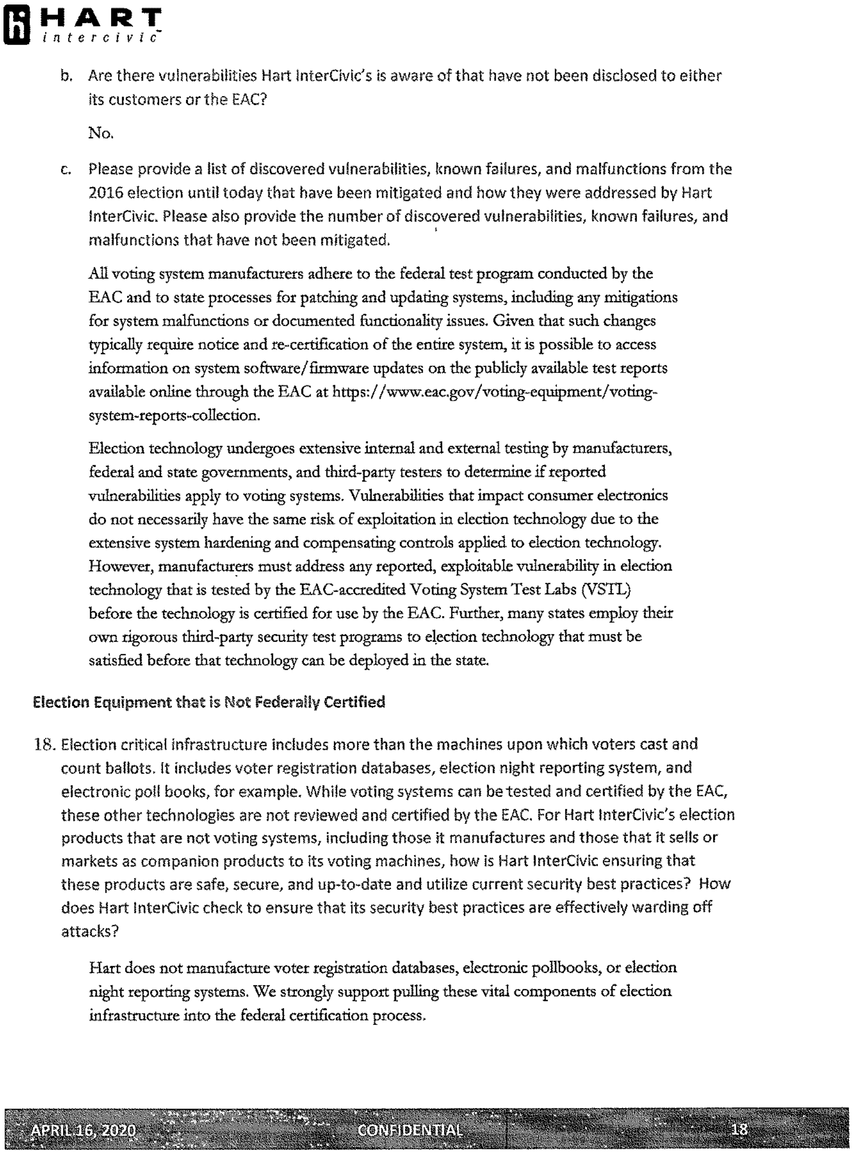
Our process to deliver any upgrade, up to and including software operating systems, follows the same tightly managed process described throughout Questions #15-16.

We strive to keep costs to state and county election officials as low as possible, however, depending on a jurisdiction's previous hardware and software configurations, there may be some costs associated with upgrades to operating systems. Those costs vary depending on the jurisdiction's existing infrastructure, in-house technical support, and the implementation timeline based on the election calendar.

17. In Hart InterCivic's October 18, 2019 response to the Committee on House Administration's oversight letter, Hart InterCivic told the Committee that it is required to "report certain issues (i.e. malfunctions) to the EAC following each federal election."

a. Does Hart InterCivic also disclose to its customers and to the EAC vulnerabilities discovered from other sources, such as white hat hackers or adversarial testing?

Yes. The source of discovery of a potential vulnerability, while informative to the initial assessment and triage phase of our response, does not alter our Incident Response policy, as described in our response to Question #1.



b. Are there vulnerabilities Hart InterCivic's is aware of that have not been disclosed to either its customers or the EAC?

No.

c. Please provide a list of discovered vulnerabilities, known failures, and malfunctions from the 2016 election until today that have been mitigated and how they were addressed by Hart InterCivic. Please also provide the number of discovered vulnerabilities, known failures, and malfunctions that have not been mitigated.

All voting system manufacturers adhere to the federal test program conducted by the EAC and to state processes for patching and updating systems, including any mitigations for system malfunctions or documented functionality issues. Given that such changes typically require notice and re-certification of the entire system, it is possible to access information on system software/firmware updates on the publicly available test reports available online through the EAC at https://www.eac.gov/voting-equipment/voting-system-reports-collection.

Election technology undergoes extensive internal and external testing by manufacturers, federal and state governments, and third-party testers to determine if reported vulnerabilities apply to voting systems. Vulnerabilities that impact consumer electronics do not necessarily have the same risk of exploitation in election technology due to the extensive system hardening and compensating controls applied to election technology. However, manufacturers must address any reported, exploitable vulnerability in election technology that is tested by the EAC-accredited Voting System Test Labs (VSTL) before the technology is certified for use by the EAC. Further, many states employ their own rigorous third-party security test programs to election technology that must be satisfied before that technology can be deployed in the state.

Election Equipment that is Not Federally Certified

18. Election critical infrastructure includes more than the machines upon which voters cast and count ballots. It includes voter registration databases, election night reporting system, and electronic poll books, for example. While voting systems can be tested and certified by the EAC, these other technologies are not reviewed and certified by the EAC. For Hart InterCivic's election products that are not voting systems, including those it manufactures and those that it sells or markets as companion products to its voting machines, how is Hart InterCivic ensuring that these products are safe, secure, and up-to-date and utilize current security best practices? How does Hart InterCivic check to ensure that its security best practices are effectively warding off attacks?

Hart does not manufacture voter registration databases, electronic pollbooks, or election night reporting systems. We strongly support pulling these vital components of election infrastructure into the federal certification process.

Network Capabilities

19. What voting machines does Hart InterCivic sell that currently have network capabilities (e.g. WiFi capabilities or Ethernet Ports) installed or as an optional add-on? Please provide the names of the machines and the type of network capabilities.

    No Verity device allows Wi-Fi or Ethernet Port connectivity, whether integrated or as an optional add-on. Further, no Verity device supports any form of remote access.

    A single state in which we have customers, Michigan, mandates the ability to transmit unofficial results at the closing of polls. For those customers, we offer a VVSG certified and compliant device, called Verity Scan with Relay, that provides a secure transmission of encrypted data over a VPN network via an installed cellular modem.

    Verity Scan with Relay is a distinct device from our standard Verity Scan, which does not permit remote transmission of any kind and is offered to states prohibiting such support. The two devices are registered separately with the EAC and have independent manufacturing builds. Verity Scan is not upgradable to a Verity Scan with Relay.

20. Is it possible for states to purchase those devices without the network capabilities?

    Yes.

21. What steps does Hart InterCivic take to secure its voting systems from the risks associated with a network connection?

    Verity Scan with Relay is a paper-based voting system that retains paper ballots as the official record of the voter's selections. In Michigan, state law dictates that only unofficial results may be transmitted remotely. The official election results must be based on vote records that are physically delivered to the jurisdiction's election headquarters.

    To protect the unofficial results transmitted by a Verity Scan with Relay, all data is encrypted and authenticated through protocols defined in the Federal Information Processing Standard (FIPS), transmitted across a secure VPN, and delivered to an air gapped device at a jurisdiction's headquarters.

Voting System Certification

22. If Hart InterCivic does sell machines with network capabilities installed or as an optional add-on, given the risks of network capabilities, why does Hart InterCivic continue to sell machines with this capability? What does Hart InterCivic think is its responsibility to notify the customers about the risks of having network capability?

    See responses to Questions #19-21.

23. Despite the fact that in 2015 the EAC updated the Voluntary Voting System Guidelines (VVSG) by issuing VVSG 1.1, all of the voting systems that Dominion [Hart] currently sells are certified to a

fifteen-year-old standard, the VVSG 1.0. Why does Dominion [Hart] choose to certify its voting systems to VVSG 1.0 rather than VVSG 1.1?

> Hart's Verity Voting system was designed to meet or exceed the security updates included in the VVSG 1.1 standard. In fact, we have certified Verity in the state of California where the state's independent election technology standard was purposely designed to incorporate and closely mirror the security features of the VVSG 1.1. standard.
>
> Our ability to certify Verity to VVSG 1.1 has been delayed because the standard contains a single, non-security related requirement on ballot handling that does not comport with the Verity design. Despite this, we have proactively implemented the security upgrades adopted in the 1.1. standard over the 1.0 standard. We encourage the Committee to review Verity's VVSG and California certification reports to confirm.

24. When Hart InterCivic sells add-on components to its EAC-certified systems that are not EAC-certified, what steps does it take to ensure its customers know those components are not EAC-certified? Does Hart InterCivic clarify this on its marketing materials? If not, why not?

> Hart does not sell non-EAC-certified add-on components which connect to or run on our EAC-certified voting systems.

25. Once the VVSG 2.0 is in place, how long will it take Hart InterCivic to design and develop systems that meet those standards? Is it possible for Hart InterCivic to take steps now to prepare for the VVSG 2.0 to minimize the time lag?

> Hart strongly supports and has been actively engaged in the process to roll out updated national standards for election systems that better address modern security requirements. We are regular participants on calls and meetings of the EAC's Technical Guidelines Development Committee (TGDC), we attend all EAC-hosted meetings related to the VVSG, and we submitted comments on the VVSG 2.0 Principles and Guidelines. We are currently reviewing the recently released draft Requirements of VVSG 2.0 and will submit our comments prior to the conclusion of the public comment period.
>
> While the Principles and Guidelines are helpful to set the overarching goals of the VVSG, it is the Requirements and Test Assertions that will provide the technical specifications upon which new and innovative election devices can be designed, built, and certified. As the Committee is aware, the Requirements have just been released and the timeline to release the Test Assertions for public review and comment is unknown at time we submitted this QFR response. Without a timetable for when the full VVSG 2.0 standard, including Test Assertions, will be released, we are not able to predict when we may have a compliant system ready for certification.
>
> We share Congress' frustration over the slow adoption of the new standards. In the meantime, we have continued to proactively enhance the security protocols of our

products to ensure that we are not stagnant on critical security enhancements while waiting on the final release of the VVSG 2.0 standard.

Further, we encourage Congress and the EAC to continue exploring ways to apply federal oversight on all election technology, including areas of high vulnerability such as voter registration systems, electronic pollbooks, and election night results reporting.

Adversarial Testing

26. What adversarial testing does Hart InterCivic perform on its voting systems? Please provide details and examples, including a list of the versions of the voting systems Hart InterCivic is currently selling that have gone through third-party adversarial testing.

Every version of Verity has gone through multiple, extensive rounds of testing, including adversarial penetration testing. Hart has submitted Verity to the federal VVSG testing and certification process (including cybersecurity and penetration tests performed by the EAC-approved testing laboratories), the robust California "red team" testing program required for state certification, and to DHS' penetration testing program run through the Idaho National Labs (INL).

As previously described in our responses to other recent inquiries from this Committee, we recognize that a proactive approach to discovering and remediating potential vulnerabilities in voting systems is critical to reducing risk in the current threat environment. It is a driving factor behind our joint industry effort to create a coordinated vulnerability disclosure program via the IT-ISAC.

As a federally regulated provider of voting systems, we have both voluntary and compulsory testing performed on every system in use as part of mandatory federal and state certification processes. Multiple factors determine whether a red team engagement is conducted as part of this testing, including customer and certification requirements. Generally, penetration testing is used to identify and remediate vulnerabilities in products before they are certified for use. However, both federal and state election authorities re-examine systems as needed.

Full end-to-end system integration tests, as well as regression test suites, are executed prior to entering the certification process. Additional tests, such as stress, volume, and security testing, address the components collectively.

The authority to require red team and or penetration-type testing currently resides largely with the states that would use it for certification purposes. However, as the Committee is aware, the EAC and NIST are working to update the federal VVSG standard and have released draft information that indicates support for a more rigorous cybersecurity testing framework at the federal level for voting systems.

Finally, we also engage in voluntary vulnerability testing services available through DHS. We've completed the penetration testing program through INL, and have also engaged in multiple tabletop exercises hosted by DHS in partnership with state, local, tribal, and territorial governments. The exercises provide attack simulations created to measure and improve an organization's staff, networks, applications, and physical security controls to withstand real-life attacks.

27. Without providing details about specific vulnerabilities in Hart InterCivic's system, what can Hart InterCivic share about what it has learned from adversarial testing?

Adversarial tests are an essential tool in uncovering vulnerabilities, setting the prioritization of remediation of those vulnerabilities based on exploitability and impact, and meeting compliance with voting industry standards.

Through adversarial and penetration testing, voting system manufacturers examine our full defensive posture against real-world, skilled human attackers. Where security assessments and audits are typically only checks against the existence of required technical controls, adversarial testing sets actual humans against our systems to actively exploit vulnerabilities to assess their impact on the systems and on our business operations.

Across multiple rounds of adversarial testing at both the state and federal level, we have been extremely pleased with Verity's resilience. The observations and assessments have been a strong validation of the forethought and effort put into our Defense in Depth security strategy from the earliest stages of product conception.

28. In addition to the adversarial testing Hart InterCivic has performed on its systems, there are independent election security researchers that test its voting systems. In the Coordinated Vulnerability Disclosure Program white paper, Hart InterCivic and other vendors in the industry indicated a desire to "vet" researchers.[3]

a. Some have said the industry's desire to place limitations on who can test its systems calls into question its commitment to truly open-ended public vulnerability testing. How does Hart InterCivic respond?

We believe a coordinated vulnerability disclosure (CVD) program for voting systems is a necessity for the elections industry, which is why we're helping lead an industrywide effort to design and deploy a program with the guidance and support of the IT-ISAC (EI-SIG).

As described in greater detail in the white paper referenced in this question, the primary challenges in developing a CVD program for election systems are related to the design of the devices and the election process itself, rather than manufacturers' desire to hand-select the researchers who would test the devices. For example, voting devices are designed to operate on closed, isolated networks which poses a unique challenge to standard models of crowd-sourced security efforts. Because the devices are not connected to the internet, it is impossible to upload a voting machine to a secure

[3] *Coordinated Vulnerability Disclosure Program White Paper*, page 3, available at: https://docs.wixstatic.com/ugd/b8fa6c_112b6b0bdc764533816b57dfdb3481b9.pdf.

platform for researchers to perform their investigations without creating new vulnerabilities and security risks. Further, the parameters of an elections industry CVD program require researchers who accept that the timing of public disclosures may necessarily be delayed in the name of election integrity. Common practice among security researchers dictates public disclosure of a discovered vulnerability in typically no more than three months from time of notification – a standard that would barely cover the timeline for federal certification, much less state certification and deployment. Unless researchers agree to a greatly extended reporting schedule – which could lag up to a year, given state certification timelines – we risk exposing potential vulnerabilities months before a solution can be implemented, and likely during live elections, which could have a direct negative impact on voter confidence and participation in our democratic process.

Despite these challenges, we are confident the elections industry, in partnership with the IT-ISAC (EI-SIG), will deploy a CVD program that grants access to ethical researchers without unduly risking the integrity of elections.

b. Has Hart InterCivic ever taken steps, such as threatening legal action, to try to prevent independent researchers from testing or gaining access to its products? If so, please provide details and explain why Hart InterCivic wants to prevent this testing.

Hart has never initiated a lawsuit or legal challenge against an independent researcher.

c. Is it Hart InterCivic's position that the modification, execution, possession, or transfer of its elections systems software by an individual without its consent using otherwise lawfully possessed or owned election systems hardware is a copyright infringement?

Though the legality of such a situation would depend on the specific activity, it is our intention to work with – rather than initiate a legal challenges *against* – any ethical researcher who contacts Hart in good faith to inform us of a potential security vulnerability that may impact any of our systems or operations.

Revenue and Investment

29. What percentage of Hart InterCivic's revenue in fiscal years 2019, 2018, and 2017 did it invest in research and development? Please provide the percentage by year.

Although industry revenues vary significantly year-to-year, nearly a third of our staff – representing the largest resource investment across the entire company each year – is dedicated to research and development of our Verity Voting system. Since Verity's initial debut in 2015, we have maintained a consistent focus on innovation, security enhancements, and product improvements.

Verity is the newest, and in our opinion, most secure election system on the market. Significant resources and funding were dedicated to Verity's design and launch, and we continue to reinvest in Verity each and every year.

30. Taxpayer dollars are used to purchase Hart InterCivic's voting machines. It is important for taxpayers to know how the investment in research and development compares with the compensation of Hart InterCivic's executives. How much money in fiscal years 2019, 2018, and 2017 went to compensating senior management? What percentage of Hart InterCivic's revenue did that constitute?

   Our top priority, driving every operational and fiscal decision in our business, is providing election officials with voting devices that meet or exceed their standards for accessibility and security. As described in our response to Question #29, and throughout this QFR, Hart consistently invests significant resources into our innovative Verity Voting system.

31. During the hearing, Ms. Mathis confirmed that Hart InterCivic has private equity investors. What role does Hart InterCivic's private equity investors play in the direction setting of Hart InterCivic's policies and procedures?

   Hart is run and managed by our executive leadership team in Austin, Texas. While representatives of our private equity investor serve on Hart's board of directors, all decisions on company policy and procedure are made locally by Hart leadership.

Paper Records in Voting

32. During the hearing, Ms. Mathis testified that Hart InterCivic continues to sell a paperless DRE machine called the "Verity Touch," but she assured the Committee that it is secure.

   a. What steps does Hart InterCivic take to ensure that the Verity Touch is secure?

      We know there is no single tactic or protocol, however robust, that can guard against every possible challenge to election security, especially over time. So rather than investing our cyber defense efforts in any singularly focused strategy, we believe the best approach to security in election technology must tightly knit people, processes, and procedures along with technology. This philosophy impacts how we view the defense posture across our entire Verity Voting system.

      To protect the integrity of every vote cast on a Verity device, including Verity Touch, we apply a layered, Defense in Depth approach to security that addresses the shifting gamut of potential vulnerabilities in both the technology and human controlled processes of voting. By implementing multiple layers of security controls, of different types, we maximize defenses and reduce gaps between those defenses. Even the most secure voting systems may fail if not backed up by officials who are focused on security and have the relevant and timely knowledge they need to deploy best practices.

      By applying Defense in Depth to each aspect of election preparedness – people, processes, procedures, and technology – we are able to build a strong security framework with multiple, independent and redundant layers of protection and readiness.

The security features of all Verity devices, including Verity Touch, include:

- All Verity devices are air gapped and physically prevented from accessing a network wired ethernet port or Wi-Fi connectivity.
- Remote access is strictly prohibited by design.
- Physical security of the devices is enhanced through port obfuscation, locked and sealed compartments for Verity drives, tamper-evident seals, and strict chain-of-custody protocols.
- Immutable audit logs record who accessed the system and what actions were performed.
- Verity employs a Triple A security model – authentication, authorization, and accounting – that runs separately from the host operating system and the jurisdiction's infrastructure.
- Two-Factor Authentication is required across the Verity Voting system.
- Application whitelisting runs on every Verity component, preventing any unauthorized or altered programs or code from being executed.
- Data validation occurs at all system boundaries to prevent any attacks via malformed inputs, SQL injection, and other data input threats.
- Transport Layer Security (TLS) protects all local network communication between Verity components which are closed-network capable (e.g. election office workstations).
- Strict firewall protocols are enabled to reject communications originating from an unauthorized source.
- Verity is configured to operate exclusively on a private network which is designed to be incapable of communicating within an intranet (e.g., an election office's public network) or the internet (e.g., a global, public network).
- All user and system actions are logged and auditable.
- We apply NIST and VVSG compliant encryption protocols across all Verity devices.
- Verity employs a System Validation Tool that enables users to verify the hashes on all Verity software files, ensuring that the software is tamper-evident.
- Verity applies Minimal Attack Surface by running on a reduced operating system and hardware configuration to diminish potential threats.
- Verity applies the concept of least privilege – election officials can customize user roles define permissions and access for all users further reducing potential threats.

In addition to the multi-layered, redundant defense protocols detailed above, every Verity device we deliver to a local election office, including Verity Touch, is federally and state certified, has undergone rigorous testing by EAC- and state-accredited testing labs, and has passed through multiple rounds of adversarial testing.

The Committee can learn more about our Defense in Depth strategy in our white paper, "Defending the Castle: Protecting Your Elections with Defense-in-Depth" available at: https://www.hartintercivic.com/wp-content/uploads/DefenseInDepth.pdf.

b. Why does Hart InterCivic believe it is more secure than other DREs that have had security flaws exposed in the past?

See response to Question #32(a).

33. Meanwhile, there is a clear consensus among security experts that the paper ballots are needed to ensure that voters votes are counted properly. In fact, a report from the National Academies of Science, Engineering, and Medicine found that "[v]oting machines that do not provide the capacity for independent auditing (e.g., machines that do not produce a voter-verifiable paper audit trail) should be removed from service as soon as possible."[4] Furthermore, Virginia decertified all of its DREs in 2017 due to security concerns. However, during her testimony, Ms. Mathis asserted that other methods of auditing and testing could be used on these machines.

a. What method of auditing was she referring to and why does she disagree with election security experts who believe the DREs cannot be audited? Please describe the methods of auditing that can be conducted on DREs in detail.

All Verity devices are designed with immutable audit logs, verifiable digital signatures on the data recorded and stored on the device, and tamper-evident security checks to alert election officials to any unauthorized action performed on the device. Additionally, cast vote record data is stored in triple redundant locations for cross-check audits.

As described throughout this QFR response, all election devices must pass rigorous audits before deployment for an election. All election machines, for example, are subjected to logic and accuracy testing prior to and after an election, ensuring the device is accurately recording the voters' selections. Further, parallel tests – selecting a random percentage of equipment to deploy in a testing environment simultaneously to a live election – can add additional verification of the accuracy of the data recorded by the devices.

And, as more thoroughly discussed previously in this QFR, nearly all states require additional post-election audits that add another layer of assurance around the accuracy of election results.

[4] National Academies of Sciences, Engineering, and Medicine, 2018. *Securing the Vote: Protecting American Democracy*, Washington, DC: The National Academies Press., page 81, https://doi.org/10.17226/25120.

b. Why does Hart InterCivic continue to sell a machine that lacks a paper trail, which is a known security risk?

How voters cast their ballot is a policy choice best decided by the elected officials that live, work, and interact with the citizens in their local communities. Hart is committed to providing secure election technology across multiple voting styles, including hand-marked paper ballots. So long as election systems pass rigorous state and federal testing and certification and are accompanied by effective post-election audits, we stand ready to deliver voting solutions that meet the requirements and needs as determined by local officials.

c. What does Hart InterCivic think its responsibility is to notify the customers about the risks of paperless machines?

See response to Question #33(b).

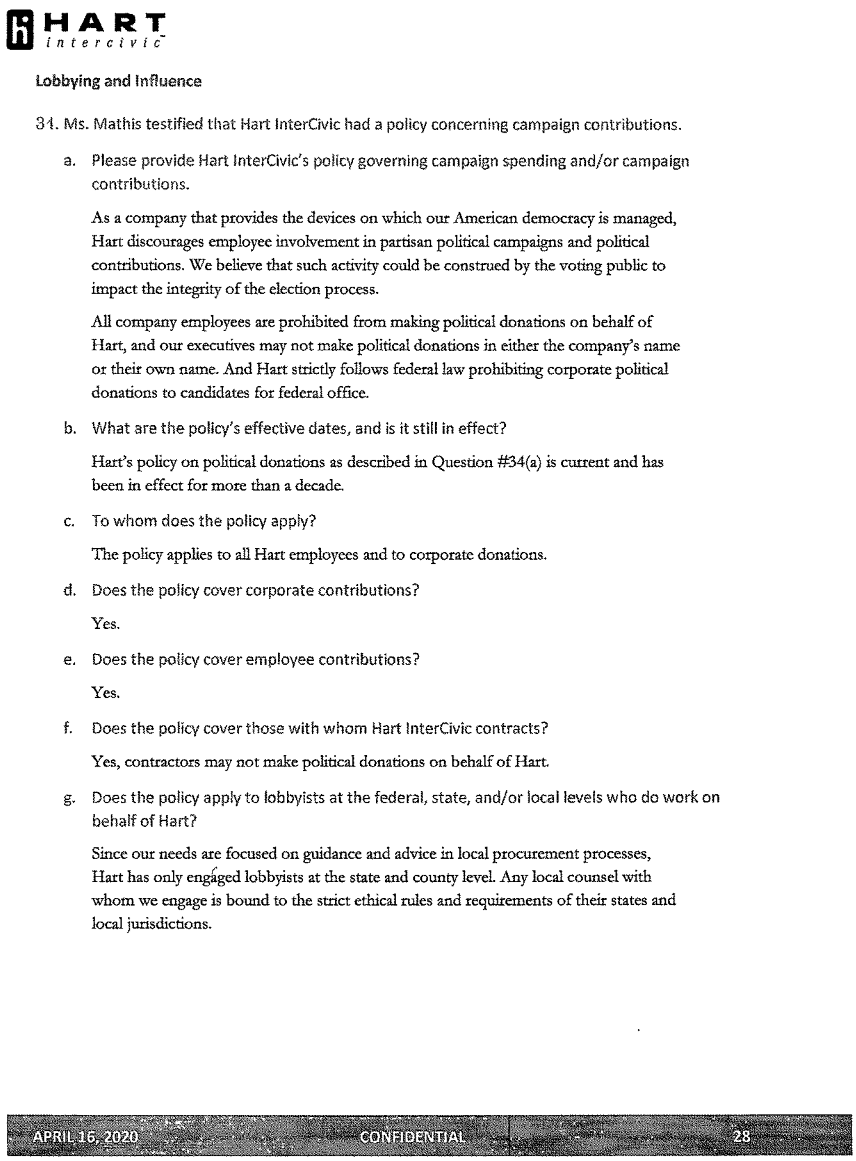
d. What are the profit margins for the Verity Touch compared to other voting machines that Hart InterCivic sells?

As the Committee heard during the hearing and in responses to previous written inquiries, margins in the election industry vary widely state-to-state and even county-to-county within a state. No one voting method is more or less profitable at a macro level.

There are numerous factors that impact industry margins, including:

- The size of the jurisdiction.
- The specific voting procedures required by the jurisdiction.
- The type of polling place set-up required.
- Specific system solution requests by jurisdictions.
- The length and cost of the state certification process.
- The training and implementation needs of the jurisdiction.
- Changes in voting equipment quantities.
- Changes in voting styles that may happen during implementations (e.g., COVID-19 is currently causing an unforeseen increase in by-mail and early voting).

We are seeing many of these factors change almost daily as states and counties scramble to adjust their traditional voting models to account for the realities of voting under the COVID-19 pandemic. As a trusted partner to our local election official customers, we are actively consulting with each of them to help plan out the most efficient and cost-effective path toward providing their voters with a safe voting experience in 2020. We stand ready to deliver reliable and secure devices that will meet localized needs at the best possible prices.



HART intercivic

Lobbying and Influence

34. Ms. Mathis testified that Hart InterCivic had a policy concerning campaign contributions.

a. Please provide Hart InterCivic's policy governing campaign spending and/or campaign contributions.

As a company that provides the devices on which our American democracy is managed, Hart discourages employee involvement in partisan political campaigns and political contributions. We believe that such activity could be construed by the voting public to impact the integrity of the election process.

All company employees are prohibited from making political donations on behalf of Hart, and our executives may not make political donations in either the company's name or their own name. And Hart strictly follows federal law prohibiting corporate political donations to candidates for federal office.

b. What are the policy's effective dates, and is it still in effect?

Hart's policy on political donations as described in Question #34(a) is current and has been in effect for more than a decade.

c. To whom does the policy apply?

The policy applies to all Hart employees and to corporate donations.

d. Does the policy cover corporate contributions?

Yes.

e. Does the policy cover employee contributions?

Yes.

f. Does the policy cover those with whom Hart InterCivic contracts?

Yes, contractors may not make political donations on behalf of Hart.

g. Does the policy apply to lobbyists at the federal, state, and/or local levels who do work on behalf of Hart?

Since our needs are focused on guidance and advice in local procurement processes, Hart has only engaged lobbyists at the state and county level. Any local counsel with whom we engage is bound to the strict ethical rules and requirements of their states and local jurisdictions.

35. Concerning Hart InterCivic's lobbying and marketing practices and policies:

   a. What percentage of Hart InterCivic's budget was spent on lobbying in fiscal years 2019, 2018, and 2017? How much money did that constitute in dollar figures? How are those funds spent?

      As described in our response to Question #34(d), we hire local counsel to provide guidance in navigating state and county procurement processes. Hart spends less than one percent of our budget on lobbying activity.

   b. What percentage of Hart InterCivic's budget was spent on marketing in fiscal years 2019, 2018, and 2017? How much money did that constitute in dollar figures? How are those funds spent?

      Like all American companies, Hart's marketing budget is spent to achieve several goals. First, to introduce Hart and our Verity Voting system to potential customers across the country. Second, to engage with those customers to better understand their needs and restrictions, in order that we can craft an individualized voting system solution that best fits the needs of their jurisdiction. And finally, to communicate timely and accurate information to customers, including sharing best practices on election processes and security through training videos, webinars, and newsletters.

      Less than five percent of our budget is dedicated to this regular communication with our customers across the nation.

   c. Please provide a list of jurisdictions in which Hart InterCivic has registered lobbyists.

      Hart has counsel on retainer to guide us through state and county procurement processes in three states: Louisiana, Ohio, and Texas.

36. According to a June 2018 McClatchy article, ES&S maintained at the time a "Board of Advisors" comprised of election officials that are responsible for negotiating and awarding voting system contracts.[5]

   a. Does Hart InterCivic now or has it ever maintained a similar customer board?

      No.

   b. If so, please provide a list of all past and present members.

      N/A.

   c. Does Hart InterCivic pay for travel and entertainment for this board to attend meetings about Hart InterCivic products? Please provide details.

      N/A.

[5] Greg Gordon, et al. "Voting machine vendor treated election officials to trips to Vegas, elsewhere," *McClatchy* (June 21, 2018) https://www.mcclatchydc.com/latest-news/article213558729.html

Unsigned Code

37. In response to Chairperson Lofgren's question: "Do all of your election systems currently in use prevent unauthorized code or altered operating systems from running on them in this way?" Ms. Mathis responded: "Our Verity product line actually incorporates a feature called white listing which actually only allows the programs that we permit with our Verity design, so it actually blocks everything except for those."

    a. Does Hart InterCivic have elections systems other than its Verity product line that are currently in use? If so, do these systems also prevent unauthorized code or an altered operating systems from running on?

    To best safeguard any older election equipment still in the field, we maintain regular contact with our customers, routinely conducting webinars and releasing best practice reports on proper maintenance of Hart voting systems, chain-of-custody procedures, and the latest technical security guidelines and practices.

    We believe it is our responsibility to alert and educate local election officials to the latest trends in elections security. Our Defense in Depth approach to security goes beyond technology. As described throughout this response, the people and processes in election administration are essential safeguards of our democracy. Through routine outreach and education across our customer base, we hope to mitigate potential threats before they can take root. In many cases, this is a frank discussion that the best way to secure a jurisdiction's voting process is a move to a modern election system.

    b. Regarding Hart InterCivic's Verity product line, can Hart InterCivic please provide to the Committee a whitepaper or more technical description of how exactly Verity's whitelisting works? Disclosure of such details is common practice among computer and smartphone vendors, who have both publicly disclosed technical details of how their secure boot and code signing/whitelisting protections work.

    As described during the hearing and previously in this QFR response, Hart has applied Application Whitelisting to every component in our Verity Voting system.

    The Whitelisting process prevents all unauthorized programs or code from being executed by reviewing and authenticating the hash of the software programs prior to execution. Stated another way, if any new application is added to the Verity software suite, or any existing application is modified or tampered with, it is prevented from being executed.

    A Whitelist is the inverse security approach to the once common practice of "Blacklisting" – most anti-virus/malware solutions work by maintaining a blacklist of previously identified threats and then preventing those programs from executing if present in the system. Blacklisting protects against known threats but cannot prevent unknown threats.

We believe Whitelisting provides a higher degree of security by only allowing pre-approved software to execute. For Verity, our whitelist is defined during the Trusted Build process and is protected from later modification. Verity whitelisting works in a "default deny" mode rather than the less secure method of bypassing inspection. All programs, without exception, are hash authenticated to determine if they are on the approved list of authorized executables -- and only those explicitly authorized applications may run.

We are encouraged to see that Whitelists have been proposed by the EAC as a requirement in VVSG 2.0. It is a best practice that should be adopted broadly in the election industry and we are proud to have led the way.

MINORITY QUESTIONS FOR THE RECORD

1. Could you describe in detail how some of your machines are able to assist voters with disabilities?

Hart is committed to ensure equal and independent voting for all voters, including those with disabilities. Our systems are specifically designed to meet the needs of all types of voters and to ensure those voters' ballots are no different from all other ballots.

The features in Verity that assist voters with disabilities include:

- Thorough usability testing by voters with disabilities is a critical part of the development process across all our Verity Voting devices.
- We put significant effort into forming and maintaining close working partnerships with well-established disability rights/advocacy groups who can provide unique voter insights which are then incorporated broadly into the Verity system.
- We never use "segregated" or "special" components for accessible voting -- *all* components are designed to be accessible to *all* voters and are fully integrated parts of the overall Verity Voting system. Accessibility is built into the design of the ballot marking device, the voting booth, and the ballot scanner.
- Every Verity device has been certified by the EAC to meet VVSG requirements related to ADA "Controls within Reach."
- The height, position, and orientation of all labels, displays, controls, audio jacks, and any other part of the accessible voting station are specifically designed not to interfere with wheelchair controls and arm rests, whether the wheelchair approaches frontally or laterally.
- Hart's accessible voting devices are equipped with the Verity Access audio-tactile interface (ATI), which includes tactile buttons and audio ballot capability, as well as compatibility with other adaptive devices, such as jelly switches or sip-and-puff devices. The buttons are raised, with beveled edges to facilitate tactile use, and all buttons also include raised Braille markings. In addition, the buttons are "dished" to

support voters who use mouthpieces (e.g., if the voter has a dexterity impairment or paralysis).

- Our accessible devices support a rich and user-friendly audio ballot experience for voters who are blind or visually impaired. This interface enables users to configure settings for audio volume, audio speech rate, visible magnification, contrast settings, language preference, and audio or visual ballot modes.
- Paper ballots produced by Verity accessible devices look and feel just like the paper ballots cast by voters who do not utilize the accessible devices. Accordingly, all ballots are the same across the entire Verity system; there are no segregated ballots that look or feel different for certain types of voters. From the outset, this was an important philosophical design decision that Hart committed to strongly for the Verity family of technology.
- As with ballots printed for hand-marking in the Verity Voting system, each ballot produced by an accessible device is anonymous and cannot be identified by image, code, or other methods.
- The materials that Hart uses to train a customer on proper usage of the system include detailed instructions on all of the accessibility features of the voting devices.

BRENNAN
CENTER
FOR JUSTICE

HEARING
COMMITTEE ON HOUSE ADMINISTRATION
"2020 ELECTION SECURITY-PERSPECTIVES FROM VOTING SYSTEM VENDORS AND EXPERTS"
JANUARY 9, 2019
MAJORITY QUESTIONS FOR THE RECORD
FOR
MS. LIZ HOWARD
COUNSEL, BRENNAN CENTER FOR JUSTICE

1. **With three vendors controlling at least eighty percent of the voting system marketplace, it is very challenging for new vendors to enter the market:**

   a. **Do you believe that it's reasonable for the American public to be concerned about a highly concentrated election industry? Why or why not?**

   It is reasonable for the American public to be concerned about a highly concentrated election industry, as the market reach of these few companies leaves our country's election infrastructure highly vulnerable to disruption.

   The current marketplace structure fails to provide sufficient incentives to ensure that the election industry will invest in cybersecurity best practices. As a general rule, competition not only ensures low prices; it ensures that the quality of products offered by these private companies is high.[1] In a relatively closed marketplace, the traditional economic motivations of competition dissipate, and companies are left with fewer incentives to improve the quality of their product in order to gain a

[1] See generally Carl Shapiro, "Competition and Innovation: Did Arrow Hit the Bull's Eye?," in *The Rate & Direction of Economic Activity Revisited*, National Bureau of Economic Research (2002), https://www.nber.org/chapters/c12360.pdf.

competitive advantage. This is evident in the current election marketplace.[2] Without adequate competition, private companies have had little incentive to improve their cybersecurity practices; these measures were simply not necessary to attract more election officials as customers. This had led to an overall underinvestment in cybersecurity in the private election infrastructure industry. And the lack of federal oversight only exacerbates these problems.

With the responsibility for administering elections spread across more than 8,000 local election jurisdictions, our decentralization is often pointed to as a key strength for election security. But this strength is diminished when the technology used to administer elections is provided by only a handful of private vendors. The ability of a malicious actor to exploit the vulnerabilities of a single vendor could have extraordinary repercussions for election security across the entire country. When election vendors fail to take the steps necessary to protect the security of their operations and equipment, they put the public confidence in our democratic system at risk.

b. Do you believe that a relatively closed marketplace with high barriers to entry ensures adequate choice for our nation's election officials? Why or why not?

The closed marketplace for voting equipment leaves election officials with little choice in selecting vendors or bargaining for preferred election infrastructure.

The lack of vendor choice may constrict the ability of election officials to find equipment that meets their specific county needs. The decentralization of election administration means that there is considerable variation in election procedures and priorities from jurisdiction to jurisdiction. But the lack of competition in the marketplace means that too often state and local governments are forced to select among one-size-fits-all equipment. Jurisdictions are often forced to adjust their procedures to the demands of available technology rather than the other way around.

[2] *The Business of Voting: Market Structure and Innovation in the Election Technology Industry*, Penn Wharton Public Policy Initiative, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-votin.

The closed marketplace also leaves election officials without significant bargaining leverage in contracts. Current industry practices favor long-term deals which require the ongoing purchase of specific vendor-approved equipment.[3] Although servicing and maintenance contracts may be optional, the specialized nature of these machines means that election officials are effectively forced to return to the vendor for maintenance of these technologies. And beyond the ongoing costs of exclusivity, election officials also lack the power to negotiate favorable terms that would boost election security efforts, such as mandatory reporting of security incidents or assurances that the company will meet internal security best practices.[4] While election officials in large counties may have greater leverage and funding to demand specific innovations, most election officials simply do not have the resources to do so.

c. How can the current market structure better support innovation and choice, or are changes required and if so, what would you recommend?

Congress could support innovation and choice in the election market by: (1) establishing comprehensive cybersecurity regulations for election vendors so that officials could choose products with confidence, and (2) providing consistent federal funding for election equipment.

First, Congress should create a new federal certification program for election vendors that will ensure that vendors are implementing best practices. These best practices should encourage vendors to attest that their conduct meets standards concerning cybersecurity, personnel management, disclosure of ownership and foreign control, incident reporting, and supply chain integrity. When election officials contract with certified vendors under this program, they can rely on the federal government to do its part to keep our elections safe by conducting

[3] Jessica Huseman, "The Market for Voting Machines Is Broke. This Company Has Thrived in It," *ProPublica*, October 28, 2019, https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it.

[4] Christopher Deluzio, *A Procurement Guide for Better Election Cybersecurity*, Brennan Center for Justice, 2019, https://www.brennancenter.org/our-work/policy-solutions/procurement-guide-better-election-cybersecurity.

ongoing oversight of these vendors. This confidence would lower information costs for election officials and open up a broader range of options beyond the companies with the most name recognition. Election officials would also gain greater bargaining power and would be relieved of the pressure to demand these security best practices in contractual terms.

Second, Congress should increase federal funding and provide a consistent stream for states and local governments to purchase and maintain election equipment. A dependable stream of funding would give election officials greater ability to shop-around and would create less pressure to enter into long-term maintenance contracts. It would also create a greater incentive for start-ups to enter the market knowing there will be reliable demand.

2. Congress just appropriated an additional $425 million for election security. What are the most critical vulnerabilities states should address with these funds?

The Brennan Center has identified the following four election security priorities: 1) replacing paperless and aging voting equipment, 2) upgrading or replacing statewide voter registration systems, 3) providing additional state and local election cybersecurity assistance, and 4) implementing rigorous post-election audits.

Replacing aging and paperless voting machines

The continued use of antiquated and paperless voting machines is a significant election security concern. Aging voting machines are more likely to fail and increasingly difficult to maintain. Paperless voting systems are not reliably auditable and have been identified as an unacceptable risk to the integrity of our election infrastructure by cybersecurity experts, including the National Academies of Sciences, Engineering and Medicine, national security experts and election officials.

We estimate that in November 2018, 34 percent of all local election jurisdictions were using voting machines that were at least 10 years old as the primary polling place equipment. While states have made significant improvement in replacing old voting machines since November 2018, much work remains to be done. Moreover, although the number of states using paperless voting machines has decreased by almost 50% since 2016, eight states are still using paperless systems as principal voting equipment in at least some counties and towns.

Providing additional state and local election cybersecurity assistance

Election officials at the state and local level oversee or rely on a variety of systems that work together to enable officials to effectively administer elections. These systems can include voter registration databases, email servers, firewalls, and much more. Election officials are expected to protect these systems, including the voter information maintained and the election results collected and transmitted on these systems, on an ongoing basis. However, as one state election official put it to us, "it is not reasonable" to expect each of the more than 8,000 separate election offices in the country to "defend against hostile nation state actors." This is particularly the case for local election offices who have little or no in-house IT or cybersecurity resources.

Election officials need a state program that provides election security and cybersecurity professional services to local election officials. Illinois recently developed a such a program, where cyber navigators with responsibility for geographic zones will work across the state with local election officials to train relevant personnel and lead risk assessments and evaluations, among other things. They will fill a role akin in many ways to that of a chief information security officer for counties. Their assessment and evaluation efforts will 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 and information sharing.

Upgrading or replacing statewide voter registration systems

Many statewide voter registration systems in use today were first built and deployed between 2004 and 2006 as states were working to meet the Help America Vote Act requirements. These systems were not designed with cybersecurity protections needed to face today's threats against our election infrastructure. We know that statewide voter registration systems are primary targets of foreign interference, as evidenced by the successful breach of Illinois' system and the attempted breach of Arizona's system prior to the 2016 election.

Implementing robust post-election audits

Traditional post-election audits, which generally require manual inspection of paper ballots cast in randomly selected precincts or on randomly selected voting machines, can provide assurance that individual voting machines accurately tabulated votes. Currently, only 24 states and the District of Columbia have voter verifiable paper records for all votes cast and require post-election audits of those paper records before certifying election results.

Robust post-election audits, such as risk-limiting audits (RLAs), do much more than simply confirming a few tabulators worked correctly. RLAs answer the big question, "Did the reported winner really get the most votes, as shown by the paper records?" Further, these audits are generally able to confirm accuracy of the outcome through review of a smaller number of ballots than what is required for a traditional post-election audit because RLAs rely on statistical sampling methods.

3. If states use these funds to buy new voting machines, what vulnerabilities should they avoid?

When purchasing voting machines, states and localities must avoid purchasing "voting machines that do not provide the capacity for independent auditing (e.g. machines that do not produce a voter-verifiable paper audit trail)".[5] In the face of growing cyber threats and the sophistication of adversaries, election officials should not only pay attention to what vulnerabilities to avoid when purchasing voting machines, but also what best practices to look for in the selection and management of election vendors. The Brennan Center has identified nine key areas that election officials and policymakers should consider as ways to achieve better vendor cybersecurity: source code disclosure, adequate procedures to manage personnel-related risks (insider attacks), robust security incident reporting, patching/software updates, security

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

assessments/audits, regular penetration testing, risk-limiting audit support, foreign nexus disclosure, and supply chain risk management.[6]

4. Is this enough funding? If no, why not and how much more is needed?

While the recent federal election security funding of $425 million was much needed, it is not enough to fully fund just the four election security priorities identified above. Moreover, the absence of an ongoing federal commitment to provide funds for election security limits the usefulness of these federal funds, especially in states that restrict hiring without long-term funding streams.

The nation's top election officials have stated that they need additional resources to protect our elections from cyberattacks. Although the question 'How much is enough?' is a difficult one to answer, given the fact that cyber threats evolve and change over time, and because the nation's infrastructure is vast, with needs varying greatly across more than 8,000 separate election administration jurisdictions, 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."

This estimate does not include the funds needed to create a resilient election administration infrastructure that can withstand a pandemic, such as the one we are currently facing. The Brennan Center estimates those costs to be up to $2 billion.[7]

MINORITY QUESTIONS FOR THE RECORD

1. In your written statement you say, "beyond voting machines themselves, other technologies that play critical roles in our current

[6] Christopher Deluzio, *A Procurement Guide for Better Election Cybersecurity*, Brennan Center for Justice, 2019, https://www.brennancenter.org/sites/default/files/201908/Report_ProcurementGuideForBetterElectionCybersecurity.pdf.

[7] Lawrence Norden, Edgardo Cortés, Elizabeth Howard, Gowri Ramachandran, and Derek Tisler, *Estimated Costs of Covid-19 Election Resiliency Measures*, Brennan Center for Justice, 2020, https://www.brennancenter.org/our-work/research-reports/estimated-costs-covid-19-election-resiliency-measures.

election system, like voter registration databases and electronic pollbooks, are also supplied and serviced by these and other private companies." Are these and other technologies at risk in your opinion based on what happened in the 2016 election?

a. If yes, how so?

Yes. Technology plays a greater role in our election process today than at any point in our country's history. And while this increased use of technology has had many positive effects for administrative efficiency and voter accessibility, each new introduction creates additional vulnerabilities that malicious actors could exploit if precautions aren't taken.

In 2016, Russian actors likely targeted election systems in all 50 states and breached and extracted data from at least one state registration database. If malicious actors were able to exploit vulnerabilities in voter registration databases in 2020, they could have the ability to alter or delete voter records, disrupt provisional ballot validation, and hinder resources that are dependent on the databases such as voter information lookup tools. While states have taken significant steps to secure these databases since 2016, private companies also play a significant role in the production and maintenance of these systems.

Similarly, electronic pollbooks in polling places present a security risk. Disruptions to these computers used to check-in voters could slow down the ability for poll workers to verify registration status and cause long lines on election day. Malicious actors could also cause these devices to indicate that voters had already cast an absentee ballot, inducing a similar disruption as Durham County, North Carolina experienced in 2016.[8] Electronic pollbooks have become a more significant focus of election security, as the number of in-person voters using e-pollbooks to check in for elections increased 71.9% from 2012 to

[8] Pam Fessler, "Russian Cyberattack Targeted Elections Vendor Tied to Voting Day Disruptions," NPR, Aug. 10, 2018, https://www.npr.org/2017/08/10/542634370/russian-cyberattack-targeted-elec-tions-vendor-tied-to-voting-day-disruptions.

2016 "from 645 jurisdictions in 2012 to 1,109 jurisdictions in 2016."[9] This number is only expected to increase in the 2020 election.

Election night reporting systems offer another point of vulnerability. As with registration databases and electronic pollbooks, private companies are often involved with the creation and maintenance of these systems. The public expects quick and accurate reporting of election results and has relied on the accuracy of these numbers for determining election outcomes. Erroneous election night reporting could open the door for bad faith actors to spread disinformation and undermine public confidence in the validity of elections.

Given the severe consequences of a potential security breakdown in these systems, any and all voting technology provided by private companies are at risk and adequate measures should be taken to ensure the technical integrity of these technologies.

2. **You also mention Risk Limiting Audits, specifically Colorado's, the first in the country. Please describe the following:**

   a. **How long did it take Colorado to get their audit up and running?**

It took approximately 8 years to successfully launch the first statewide risk-limiting audit in the country. The lessons learned through this process have enabled election officials across the country to quickly conduct pilot RLAs in their own jurisdictions. For example, Michigan officials conducted multiple successful pilot RLAs[10] within five months of the project launch, and Rhode Island[11] will conduct its first mandatory statewide RLA approximately two years after its first

[9] "EAVS Deep Dive: Election Technology," Election Assistance Commission, May 1, 2018, https://www.eac.gov/documents/2018/05/01/eavs-deep-dive-election-technology.

[10] Andrea Peck, "Rochester Hills to conduct post-election audit," *Oakland Press*, Dec. 2, 2018, https://www.theoaklandpress.com/news/local/rochester-hills-to-conduct-post-election-audit/article_593f0ba0-f324-11e8-9b5f-2f927d645982.html.

[11] "New Report Details Rhode Island's Risk-Limiting Audit Tests to Identify Best System for 2020 Election," *Common Cause*, Sept. 3, 2019, https://www.commoncause.org/rhode-island/press-release/new-report-details-rhode-islands-risk-limiting-audit-tests-to-identify-best-system-for-2020-election/.

successful pilot in 2019. And the free RLA tools now available have enabled election officials in Georgia, Missouri, New Jersey, Pennsylvania and Virginia to also conduct successful pilots with only a few months of planning.[12]

b. How much did it cost?

The major cost associated with Colorado's risk-limiting audit is the RLA tool, which is software that conducts the necessary mathematical analysis and other functions essential for a statewide audit. Colorado has spent in excess of $500,000 on the development and maintenance of their RLA tool. Largely because of Colorado's investment, states can access a free RLA tool or pay a very modest annual fee of approximately $17,500 – 45,000[13] for a hosted Software-as-a-service version of an RLA tool.

Moreover, "The costs to run a risk-limiting audit are a small percentage of the overall cost to run an election. In other words, an RLA is quite affordable and, compared to older post-election audit methods, provides a greater degree of certainty that the outcome of the election is valid."[14]

c. How would their model differ from a state like Texas that is geographically much larger are diverse?

A state's size and diversity have little to no impact the RLA method selection process. There are three basic RLA models: 1) ballot comparison, 2) ballot polling and 3) batch comparison. The RLA method used is determined by the state's election administration system, specifically how election officials collect and retain ballots cast.

[12] Lawrence Norden, Elizabeth Howard, and Andrea Cordova, *Voting Machine Security: Where We Stand Six Months Before the New Hampshire Primary*, Brennan Center for Justice, 2019, https://www.brennancenter.org/our-work/analysis-opinion/voting-machine-security-where-we-stand-six-months-new-hampshire-primary.

[13] "Risk-Limiting Audits with Arlo," Voting Works, https://voting.works/risk-limiting-audits/.

[14] "Risk-Limiting Audits," RiskLimitingAudits.org, https://risklimitingaudits.org/.

In Colorado, the main method to collect ballots is by mail. This enables election officials to sort, process and tabulate ballots at a central location, which enables officials to retain and store the ballots in the same order in which they were tabulated. By retaining this order, election officials can compare the tabulator's internal record indicating how Vote #55 was counted (e.g., one vote for Margaret for Senator, one vote for Harsha for Governor) to the markings on the 55th ballot in a specific stack of ballots to check that they match how the vote was tabulated. This ability is required for ballot comparison audits.

Since most states, such as Texas and Michigan, rely primarily on votes cast in-person on a tabulator attached to a secure collection box, it is not possible to retain the ballots in the same order tabulated. These states can use the ballot polling method. For this method, a random sample of ballots is counted by hand, and these results are entered into the RLA tool. The RLA tool analyzes the results and determines whether the sample provides sufficient evidence that the reported winner actually received the most votes as reflected in the paper ballots. Our report, A Review of Robust Post-Election Audits,[15] provides additional information about the different types of RLAs and what election officials should consider before selecting an RLA method.

The batch comparison method can be used in states where the ballots cast in each precinct are separately tabulated, if those ballots are stored together. For this method, a random sample of precincts, or batches, is counted by hand, and these results are compared to the tabulated results for each batch. The results would be entered into a RLA tool for an analysis of whether the sample provides sufficient evidence that the reported winner actually received the most votes as shown by the paper ballots.

d. How many different types of audits are there currently?

There are a large number of post-election audit types. Our report, A Review of Robust Post-Election Audits, provides additional information

[15] Elizabeth Howard, Ronald L. Rivest, Phillip B. Stark, *A Review of Robust Post-Election Audits*, Brennan Center for Justice, Nov. 2019, https://www.brennancenter.org/our-work/research-reports/review-robust-post-election-audits.

about the different types of RLAs and Bayesian audits, and what election officials should consider before selecting a post-election audit method.

Separately, NCSL provides a list of other types of post-election audits.[16]

[16] See "Post-Election Audits," National Conference of State Legislatures, last updated Oct. 25, 2019, https://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx.

HEARING
COMMITTEE ON HOUSE ADMINISTRATION
"2020 ELECTION SECURITY-PERSPECTIVES FROM VOTING SYSTEM VENDORS AND EXPERTS"
JANUARY 9, 2019
MAJORITY QUESTIONS FOR THE RECORD
FOR
DR. JUAN GILBERT
ANDREW BANKS FAMILY PREEMINENCE ENDOWED PROFESSOR & CHAIR, UNIVERSITY OF FLORIDA

1. With three vendors controlling at least eighty percent of the voting system marketplace, it is very challenging for new vendors to enter the market.

    a. Do you believe that it's reasonable for the American public to be concerned about a highly concentrated election industry? Why or why not?

        i. I'm not sure what difference it would make if 3 or 5 more vendors entered the market. Would it improve anything? I don't know. The 3 are using similar technologies that have been certified. I guess the 1 possible advantage I can think of is maybe cost will go down for the States. Introducing more vendors may not increase innovation. Furthermore, I don't see very many incentives for others to enter this market.

    b. Do you believe that a relatively closed marketplace with high barriers to entry ensures adequate choice for our nation's election officials? Why or why not?

        i. No, this doesn't ensure adequate choice for election officials. If there were more competition/options in the market, then the officials would have more choices. Again, I am not sure if this would result in new voting innovations that improve elections because everyone is certified by the same standards, so most of the market is similar with respect to technology.

    c. How can the current market structure better support innovation and choice, or are changes required and if so, what would you recommend?

        i. The current market struggles with the high price and long delay of certification. The cost and time investment of the current certification process is an impediment to innovation, in my opinion. I don't know how much innovation is being explored by any of the vendors at this time because I don't see an incentive to innovate. The cost tradeoff of innovation probably isn't in their best interest. I think innovations that come from research labs would have a bigger impact. We created an open source, universally designed voting system called Prime III. This technology has been implemented in current voting technologies and the vendors are using aspects of Prime III's design. This was no cost to them, but it has a tremendous impact on the market and making elections more accessible, usable and secure. I would recommend that Congress look at recommendation 7.3 from the National Academies report, "Securing the Vote: Protecting American Democracy" This recommendation supports the establishment of a national research center with the primary focus of research and development in elections technology. This is how innovation in the market would really move forward. The vendors are unlikely to invest in risky innovations, where such a center could do the necessary research and development to advance the state of the art in elections.

2. In the absence of the VVSG 2.0, what are the most important things vendors and states can do in the lead up to the 2020 election to ensure the election is secure and voters are not disenfranchised because of malfunctioning equipment?
    a. Use paper based systems for all elections. I also recommend risk-limiting audits as well. Train poll workers on the technologies being used for elections and also train them to educate and help voters with the technologies. For example, poll workers should remind voters to verify their ballots produced by a ballot marking device.

Minority Questions for the Record

1. You mentioned in your testimony under and over vote fraud associated with hand marked paper ballots. What are examples of this?
    a. As my colleagues in cybersecurity would say, "just because no one has been caught hacking a system, doesn't mean it didn't happen", but here's an example, https://www.miamiherald.com/news/politics-government/election/article111029767.html

   b. The overvote and undervote hacks that I described in my testimony are viable hacks and could happen in any hand-marked paper ballot election. If no one is watching, this hack is impossible to detect and correct.

2. As a professor at the University of Florida, a state with a deep history of voting issues, specifically around the passage of HAVA, how would you recommend updating this law?
   a. I think a commission should be established to evaluate HAVA. Much like the National Academies consensus committee, a committee of relevant experts and stakeholders should be formed to review HAVA and make recommendations for changes to HAVA. However, I will say, HAVA funding to the States needs to continue and the U.S. Election Assistance Commission (EAC) is a necessity as well.

HEARING
COMMITTEE ON HOUSE ADMINISTRATION
"2020 ELECTION SECURITY-PERSPECTIVES FROM VOTING SYSTEM VENDORS AND EXPERTS"
JANUARY 9, 2019
MAJORITY QUESTIONS FOR THE RECORD
FOR
REV. T. ANTHONY SPEARMAN
PRESIDENT, NORTH CAROLINA NAACP

1. As a local election official, what have been the main challenges that you have experienced working with voting machine vendors?

The main challenge that I have experienced working with voting machine vendors is their aggressive and too oftentimes unethical approach to ensure that they sell their product, almost by any means necessary. They are extremely competitive. Often I have observed vendors as they provide misinformation, and intentionally fail to provide vital information that the public has a need to know. There is virtually no oversight which raises a host of concerns.

March 13, 2020

Chairwoman Zoe Lofgren
Committee on House Administration
1309 Longworth House Office Building
Washington, DC 20515

Dear Chairwoman Lofgren:

Thank you for the opportunity to appear before members of the Committee on House Administration for your hearing on January 9, 2020 entitled "2020 Election Security-Perspectives from Voting System Vendors and Experts."

I appreciate the opportunity to address how the U.S. Election Assistance Commission is fulfilling its mission to support election administrators and the voters they serve. I respectfully submit for the record the following responses to the Committee's follow-up questions.

This letter addresses each of the questions posed by the Committee's majority and minority members. Unless otherwise noted, I am solely responding to the questions as Vice Chair of the Commission. The responses do not reflect the views of my fellow Commissioners.

The EAC looks forward to our continued work together on assisting election officials across the United States in providing secure, accessible, and accurate elections.

Sincerely,

Donald Palmer, Vice Chairman

HEARING
COMMITTEE ON U.S. HOUSE ADMINISTRATION
"2020 ELECTION SECURITY-PERSPECTIVES FROM VOTING SYSTEM VENDORS AND EXPERTS"
JANUARY 9, 2020

MAJORITY QUESTIONS FOR THE RECORD
FOR THE HONORABLE DONALD PALMER
COMMISSIONER, ELECTION ASSISTANCE COMMISSION

1. In the Election Assistance Commission's (EAC's) response to an oversight letter the Committee sent in November 2019, the EAC informed the Committee that it had never decertified a voting machine. The only time the EAC mentioned that it began the process, the machine was withdrawn voluntarily by the voting machine manufacturer from the list of EAC-certified voting systems. Given the existence of machines that continue to be used long after their vulnerabilities have been exposed, why has the EAC only once begun the process of decertifying a machine?

   The EAC takes the decertification of voting systems very seriously. Decertification has the potential to impact jurisdictions that depend on these systems to run their elections. Affected jurisdictions may not have the financial means to quickly replace problematic systems with more modern versions. Section 7 of the Voting System Testing and Certification Manual (hereinafter, the "Manual") details the process of decertification including informal and formal investigations, notices of non-compliance to a manufacturer, and final decertification. The process is designed to incentivize manufacturers to fix a reported non-compliance rather than decertifying a system first with the expectation that it will be replaced with a compliant system by a jurisdiction who may not have the means to immediately do so. The EAC's Testing and Certification Program also includes a strict quality monitoring program to ensure manufacturers and users of field-certified systems maintain the certified configuration of the systems, address any manufacturing quality problems, and report field performance issues.

   According to Section 7.1 of the Manual, decertification is initiated when the EAC receives information that a voting system may not be in compliance with the Voluntary Voting System Guidelines (VVSG) or the procedural requirements of the Manual. In practice, that means that a jurisdiction or other agent must report a non-compliance before the EAC begins any informal investigation. If the EAC determines there is potential non-compliance, a formal investigation is conducted which may lead to subsequent decertification.

   The EAC has been notified of a non-compliance in the single case mentioned in our previous response and, it is the only instance of a decertification investigation that we can offer. The EAC closely monitors election system vendors and solicits information from state and local election officials on any anomaly that may appear, and remains committed to a robust, transparent, and results-driven testing and certification program.

2. In the EAC's August 12, 2019 response to the Committee's Questions for the Record, the EAC stated it would not certify a machine running an operating system that was no longer supported for security patches, but also would not decertify a machine that when the parent company of an operating system ceased to put out security patches because it would not meet the grounds for decertification under Section 7 of the Voting System Testing and Certification Manual.

    a. What provision in Section 5 of the Voluntary Voting System Guidelines (VVSG) 1.0 Volume 1 prevents a voting system running an operating system that is no longer supported for security patches from being certified?

       The EAC voting system testing and certification program does not currently have a provision to prevent a system running an operating system that is no longer supported for security patches from being submitted for certification. While the current availability of support for an operating system is not directly addressed as part of the VVSG, including the draft VVSG 2.0 requirements, the adoption of VVSG 2.0 requires updating the Testing and Certification Manual used to administer the program. The EAC envisions updates to the Manual that directly address the circumstances under which a system will be accepted for certification testing including the submission of systems using operating systems that are no longer supported with security updates. Approval of the VVSG 2.0 guidelines and updated program manuals is expected by the end of this year.

       It is important to note that in November of 2019, the EAC's Testing and Certification Program issued a Notice of Clarification providing clear guidelines on submitting minor software changes for certification. The EAC expects that this process will be used often by vendors to rapidly update the security of their systems with the latest software patches and operating system updates. To date, one vendor has utilized this new capability. The vendor's submission was approved in four days. We look forward to further utilizing this service to assist the elections community.

    b. According to the decertification policy outlined in Section 7 of the Voting System Testing and Certification Manual, one of the reasons voting systems can be decertified is if "they are shown not to meet applicable Voluntary Voting System Guidelines standards." How is it possible for a system to fail to meet the standard to be certified under the VVSG but not meet the grounds to decertify? Specifically, how is it possible that the EAC would not certify an operating system that is no longer supported for security patches, but also say that the system does not meet the grounds for decertification?

       The EAC voting system testing and certification process currently evaluates systems by determining if they are in accordance with the VVSG requirements in place at the time of certification. As mentioned in the response to question 1, the EAC has not historically pursued decertification of systems unless there is an external request to do so.

Furthermore, decertification of systems must be conducted with deliberation as it has the potential to severely impact jurisdictions and their ability to successfully run an election.

The current Manual describes a process that is meant to hold manufacturers accountable for the correct functioning, durability, and reliability of their systems. The decertification process is designed to give manufacturers an opportunity to correct defects as they are reported, not to immediately disable systems. Section 2.3.2.7 of the manual is an example of a requirement for manufacturers to submit reports on any malfunctions of EAC-certified systems when the malfunction occurs during a federal election. The manual is being updated as part of VVSG 2.0 approval and adoption with completion of the updates expected by the end of 2020. The EAC is committed to a comprehensive, transparent, and results-based testing and certification program. We look forward to the assistance that VVSG 2.0 will provide for election system vendors and others across the elections community.

MINORITY QUESTIONS FOR THE RECORD

1. We know that the Commission has and is doing everything it can to secure our elections into 2020, what new programs or initiatives is the Commission undertaking to address emerging threats?

   The EAC greatly appreciates the increased fiscal year 2020 appropriations provided by Congress. As the only federal agency committed to the whole of election administration, the EAC is focused on providing more resources to state and local election officials to help them strengthen cybersecurity practices and securely manage their election technology assets. Currently, the EAC is distributing the recent Congressional appropriation of 2020 Help America Vote Act (HAVA) funds. We will continue to work with states as they use these funds to replace aging voting equipment and bolster the security of election systems.

   In addition, the EAC is moving forward with approval of the Voluntary Voting System Guidelines (VVSG) 2.0. The Guidelines will further secure election systems and future machine development by providing updated guidelines for the certification of voting systems. It is our hope that VVSG 2.0 will receive final approval later this year.

   Regarding other vital activities, we are filling critical staffing vacancies within the agency as well as enhancing our staff to meet rising demands. The Commission recently hired two crucial security-focused positions of Deputy Chief Information Security Officer (CISO) and Senior Cybersecurity Program Manager. Both positions require in-depth security credentials as well as election technology and operations expertise. These individuals will begin developing cybersecurity capabilities to assist state and local jurisdictions with securing their election systems and programs as well as improving the overall security posture of the Commission itself.

We also plan to add staff to our Testing and Certification Program. Expansions to this program will enhance its capability of handling frequent voting system security updates through the de minimis process while fulfilling its other duties of conducting security training for election administrators, performing on-site audits of voting system manufacturing and test lab facilities, conducting field reviews of EAC-certified voting systems, support penetration testing of voting systems, and overseeing a post-election audit assistance program.

The EAC is exploring all the program areas listed below. The degree to which we are able to develop these programs is contingent on an increase in appropriations as requested. Programs the EAC would like to implement if increased funding is received:

Securing Non-voting systems

There are limited federal standards regarding the use of other types of election technology. The EAC's HAVA-mandated voluntary guidance on the implementation of statewide voter registration lists, which discusses database security measures in limited detail, has not been updated since its adoption in 2005. There are no federal standards regarding the use of electronic poll books, election night reporting systems, remote ballot delivery systems, or other computerized election systems. Given these limited standards, and the increased cybersecurity threat associated with these internet-connected systems, the EAC recognizes the importance of supporting election officials. We will work with election officials and experts to develop and share best practices and voluntary guidance in this area, as well as pilot a verification program for non-voting system election technology.

The EAC is working alongside federal partners and other stakeholders to support election officials as they seek to protect voters against disinformation in elections and promote trusted sources of information. In America's hyper-decentralized election system, where many voters are unaware of which office administers elections in their jurisdiction, it can be a challenge to provide voters with official information on registration and voting procedures. We would like to work on improving voter-facing information on vote.gov and the EAC website, as well as engage in promotional activities supporting anti-disinformation campaigns, such as #TrustedInfo2020. The EAC recently entered into an interagency agreement with the General Services Administration regarding vote.gov and is participating in #TrustedInfo2020 educational efforts led by the National Association of Secretaries of State.

Clearinghouse

The EAC website is a core component of the agency's clearinghouse function. From "nuts and bolts" election administration issues, such as voter registration, ballot design, preventing long lines, and serving voters with disabilities, to emerging issues, such as election security, cybersecurity, and health emergency preparedness, the EAC website serves as a unique national platform for information and resources that can help election officials improve election administration in their jurisdictions. The EAC seeks to revamp its website and streamline how clearinghouse resources and information are organized, as well as *collect and develop new resources on issues of importance to election officials, including issues that emerge during the 2020 elections. Funds will also be used for training materials for the states and other research projects that necessitate partnerships with universities to assist with collecting important data. Additionally, the EAC will seek to compile helpful resources to assist our stakeholders with contingency planning and election best practices.*

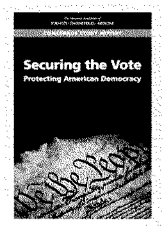
New Federal Advisory Committee for Local Election Official Leaders

With the establishment of the Election Infrastructure Subsector Government Coordinating Council (GCC) and Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), the infrastructure for national coordination and information sharing among election officials on election security and cybersecurity matters has improved significantly since 2016. The EAC Standards Board, a 110-member federal advisory committee comprised of one state and one local election official from each of the 50 states, the District of Columbia, and four U.S. territories, complements this infrastructure and provides a platform for election officials to share information and coordinate on election security and cybersecurity, as well as other election administration issues. One notable weakness of this existing national infrastructure is the limited presence of local election officials, who play the lead role in administering elections in most states.

The EAC seeks to establish and convene a 165-member federal advisory committee comprised of three local election officials from each state and territory. The local election officials represented on the advisory committee will include the president, immediate past-president, and president-elect of each state's association of local election officials. An alternative process would be used in the few states and territories where no such associations exist. This would create a body through which the EAC and its federal partners can share information quickly among local election official leaders and receive critical input and advice regarding EAC programs and activities, particularly informing discussions regarding level of resources and types of assistance most beneficial to local jurisdictions. This body would also be designed to help strengthen the profession of local election administration through the existing state association structure.

The National Academies of | SCIENCES ENGINEERING MEDICINE THE NATIONAL ACADEMIES PRESS

This PDF is available at http://nap.edu/25120 SHARE



GET THIS BOOK

FIND RELATED TITLES

Securing the Vote: Protecting American Democracy (2018)

DETAILS

180 pages | 6 x 9 | PAPERBACK
ISBN 978-0-309-47647-8 | DOI 10.17226/25120

CONTRIBUTORS

Committee on the Future of Voting: Accessible, Reliable, Verifiable Technology; Committee on Science, Technology, and Law; Policy and Global Affairs; Computer Science and Telecommunications Board; Division on Engineering and Physical Sciences; National Academies of Sciences, Engineering, and Medicine

SUGGESTED CITATION

National Academies of Sciences, Engineering, and Medicine 2018. *Securing the Vote: Protecting American Democracy*. Washington, DC: The National Academies Press. https://doi.org/10.17226/25120.

Securing the Vote

Protecting American Democracy

Committee on the Future of Voting:
Accessible, Reliable, Verifiable Technology

Committee on Science, Technology, and Law

Policy and Global Affairs

Computer Science and Telecommunications Board

Division on Engineering and Physical Sciences

A Consensus Study Report of

The National Academies of
SCIENCES • ENGINEERING • MEDICINE

THE NATIONAL ACADEMIES PRESS
Washington, DC
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, NW Washington, DC 20001

This activity was supported with grants to the National Academy of Sciences from the Carnegie Corporation of New York (#G-16-53637) and the William and Flora Hewlett Foundation (#G-2016-5031) and with funds from National Academy of Sciences' W. K. Kellogg Foundation Fund and the National Academies of Sciences, Engineering, and Medicine's Presidents' Circle Fund. Any opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of any organization or agency that provided support for the project.

International Standard Book Number-13: 978-0-309-47647-8
International Standard Book Number-10: 0-309-47647-X
Library of Congress Control Number: 2018952779
Digital Object Identifier: https://doi.org/10.17226/25120

Additional copies of this publication are available for sale from the National Academies Press, 500 Fifth Street, NW, Keck 360, Washington, DC 20001; (800) 624-6242 or (202) 334-3313; http://www.nap.edu.

Printed in the United States of America

Suggested citation: National Academies of Sciences, Engineering, and Medicine. 2018. *Securing the Vote: Protecting American Democracy*. Washington, DC: The National Academies Press. doi: https://doi.org/10.17226/25120.

The National Academies of
SCIENCES · ENGINEERING · MEDICINE

The **National Academy of Sciences** was established in 1863 by an Act of Congress, signed by President Lincoln, as a private, nongovernmental institution to advise the nation on issues related to science and technology. Members are elected by their peers for outstanding contributions to research. Dr. Marcia McNutt is president.

The **National Academy of Engineering** was established in 1964 under the charter of the National Academy of Sciences to bring the practices of engineering to advising the nation. Members are elected by their peers for extraordinary contributions to engineering. Dr. C. D. Mote, Jr., is president.

The **National Academy of Medicine** (formerly the Institute of Medicine) was established in 1970 under the charter of the National Academy of Sciences to advise the nation on medical and health issues. Members are elected by their peers for distinguished contributions to medicine and health. Dr. Victor J. Dzau is president.

The three Academies work together as the **National Academies of Sciences, Engineering, and Medicine** to provide independent, objective analysis and advice to the nation and conduct other activities to solve complex problems and inform public policy decisions. The National Academies also encourage education and research, recognize outstanding contributions to knowledge, and increase public understanding in matters of science, engineering, and medicine.

Learn more about the National Academies of Sciences, Engineering, and Medicine at **www.nationalacademies.org**.

The National Academies of
SCIENCES · ENGINEERING · MEDICINE

Consensus Study Reports published by the National Academies of Sciences, Engineering, and Medicine document the evidence-based consensus on the study's statement of task by an authoring committee of experts. Reports typically include findings, conclusions, and recommendations based on information gathered by the committee and the committee's deliberations. Each report has been subjected to a rigorous and independent peer-review process and it represents the position of the National Academies on the statement of task.

Proceedings published by the National Academies of Sciences, Engineering, and Medicine chronicle the presentations and discussions at a workshop, symposium, or other event convened by the National Academies. The statements and opinions contained in proceedings are those of the participants and are not endorsed by other participants, the planning committee, or the National Academies.

For information about other products and activities of the National Academies, please visit www.nationalacademies.org/about/whatwedo.

COMMITTEE ON THE FUTURE OF VOTING: ACCESSIBLE, RELIABLE, VERIFABLE TECHNOLOGY

Co-chairs

LEE C. BOLLINGER, President, Columbia University
MICHAEL A. McROBBIE, President, Indiana University

Members

ANDREW W. APPEL, Eugene Higgins Professor of Computer Science, Princeton University
JOSH BENALOH, Senior Cryptographer, Microsoft Research
KAREN COOK (NAS), Ray Lyman Wilbur Professor of Sociology; Director of the Institute for Research in the Social Sciences (IRiSS); and Vice-Provost for Faculty Development and Diversity, Stanford University
DANA DeBEAUVOIR, Travis County Clerk, County of Travis, TX
MOON DUCHIN, Associate Professor of Mathematics and Founding Director, Program in Science, Technology, and Society, Tufts University
JUAN E. GILBERT, Andrew Banks Family Preeminence Endowed Professor and Chair of the Computer and Information Science and Engineering Department, University of Florida
SUSAN L. GRAHAM (NAE), Pehong Chen Distinguished Professor Emerita, Computer Science Division, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley
NEAL KELLEY, Registrar of Voters and Chief of Elections, County of Orange, CA
KEVIN J. KENNEDY, Director and General Counsel (retired), Wisconsin Government Accountability Board
NATHANIEL PERSILY, James B. McClatchy Professor of Law, Stanford Law School
RONALD L. RIVEST (NAS/NAE), Institute Professor, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology
CHARLES STEWART III, Kenan Sahin Distinguished Professor of Political Science, Massachusetts Institute of Technology

Staff

ANNE-MARIE MAZZA, Study Director and Senior Director, Committee on Science, Technology, and Law
JON EISENBERG, Senior Director, Computer Science and Telecommunications Board
STEVEN KENDALL, Program Officer, Committee on Science, Technology, and Law
KAROLINA KONARZEWSKA, Program Coordinator, Committee on Science, Technology, and Law
WILLIAM J. SKANE, Consultant Writer
CLARA SAVAGE, Financial Officer, Committee on Science, Technology, and Law

COMMITTEE ON SCIENCE, TECHNOLOGY, AND LAW

Co-chairs

DAVID BALTIMORE (NAS/NAM), President Emeritus and Robert Andrews Millikan Professor of Biology, California Institute of Technology
DAVID S. TATEL, Judge, U.S. Court of Appeals for the District of Columbia Circuit

Members

THOMAS D. ALBRIGHT (NAS), Professor and Director, Vision Center Laboratory and Conrad T. Prebys Chair in Vision Research, Salk Institute for Biological Studies
ANN ARVIN (NAM), Lucile Packard Professor of Pediatrics and Microbiology and Immunology; Vice Provost and Dean of Research, Stanford University
JOE S. CECIL, Project Director (retired), Program on Scientific and Technical Evidence, Division of Research, Federal Judicial Center
R. ALTA CHARO (NAM), Warren P. Knowles Professor of Law and Bioethics, University of Wisconsin at Madison
HARRY T. EDWARDS, Judge, U.S. Court of Appeals for the District of Columbia Circuit
CHARLES ELACHI (NAE), Professor of Electrical Engineering and Planetary Science, Emeritus, California Institute of Technology
JEREMY FOGEL, Director, Federal Judicial Center
HENRY T. GREELY, Deane F. and Kate Edelman Johnson Professor of Law and Professor, by courtesy, of Genetics, Stanford University
MICHAEL IMPERIALE, Arthur F. Thurnau Professor of Microbiology and Immunology University of Michigan
ROBERT S. LANGER (NAS/NAE/NAM), David H. Koch Institute Professor, Massachusetts Institute of Technology
GOODWIN LIU, Associate Justice, California Supreme Court
JUDITH MILLER, Independent Consultant
JENNIFER MNOOKIN, Dean and David G. Price and Dallas P. Price Professor of Law, University of California, Los Angeles School of Law
MARTINE A. ROTHBLATT, Chairman and Chief Executive Officer, United Therapeutics
JOSHUA R. SANES (NAS), Professor of Molecular and Cellular Biology and Paul J. Finnegan Family Director, Center for Brain Science, Harvard University

WILLIAM B. SCHULTZ, Partner, Zuckerman Spaeder LLP
SUSAN S. SILBEY, Leon and Anne Goldberg Professor of Humanities, Professor of Sociology and Anthropology, and Professor of Behavioral and Policy Sciences, Massachusetts Institute of Technology
DAVID C. VLADECK, A.B. Chettle, Jr., Professor of Law, Georgetown University Law Center
SUSAN WESSLER (NAS), University of California President's Chair and Distinguished Professor of Genetics, University of California, Riverside

Staff

ANNE-MARIE MAZZA, Senior Director
STEVEN KENDALL, Program Officer
KAROLINA KONARZEWSKA, Program Coordinator

COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD

Chair

FARNAM JAHANIAN, Carnegie Mellon University

Members

LUIZ BARROSO, Vice President of Engineering, Google, Inc.
STEVEN M. BELLOVIN (NAE), Percy K. and Vida L. W. Hudson Professor of Computer Science, Columbia University
ROBERT F. BRAMMER, President and Chief Executive Officer, Brammer Technology, LLC
DAVID E. CULLER (NAE), Professor of Electrical Engineering and Computer Science, University of California, Berkeley
EDWARD FRANK, Chief Executive Officer, Cloud Parity, Inc.
LAURA M. HAAS (NAE), Dean, College of Information and Computer Sciences, University of Massachusetts, Amherst
MARK A. HOROWITZ (NAE), Yahoo! Founders Chair, Electrical Engineering and Computer Science, Stanford University
ERIC HORVITZ (NAE), Distinguished Scientist and Director, Microsoft Research
VIJAY KUMAR (NAE), Nemirovsky Family Dean, School of Engineering and Applied Sciences, University of Pennsylvania
BETH MYNATT, Distinguished Professor and Executive Director Institute for People and Technology, Georgia Institute of Technology
CRAIG PARTRIDGE, Chief Scientist, Raytheon BBN Technologies
DANIELA RUS (NAE), Andrew and Erna Viterbi Professor of Electrical Engineering and Computer Science and Director of the Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology
FRED B. SCHNEIDER (NAE), Samuel B. Eckert Professor of Computer Science and Chairman, Department of Computer Science, Cornell University
MARGO SELTZER, Herchel Smith Professor of Computer Science and the Faculty Director of the Center for Research on Computation and Society, Harvard University
MOSHE VARDI (NAS, NAE), Karen Ostrum George Distinguished Service Professor in Computational Engineering and Director of the Ken Kennedy Institute for Information Technology, Rice University

Staff

JON EISENBERG, Senior Director
LYNETTE I. MILLETT, Associate Director and Director, Forum on Cyber Resilience
EMILY GRUMBLING, Program Officer
KATIRIA ORTIZ, Associate Program Officer
JANKI PATEL, Senior Program Assistant
SHENAE BRADLEY, Administrative Assistant
RENEE HAWKINS, Financial and Administrative Manager

Preface

When we were asked in fall 2016 to serve as co-chairs of the committee that would ultimately author the current report, it seemed that our attention would be focused on identifying technological solutions that could redress problems such as long lines at polling places and outdated election systems. We imagined that we would offer an evaluation of the innovations being adopted by forward-looking election administrators across the nation. We suspected that we would find that voting systems are moving away from in-person physical balloting toward systems that embrace technologies that enable remote (Internet) voting.

However, by the time the committee met for the first time in April 2017, it was clear that the most significant threat to the American elections system was coming, not from faulty or outdated technologies, but from efforts to undermine the credibility of election results. Unsubstantiated claims about election outcomes fanned by social and other media threaten civic stability. Perhaps even more troubling is evidence that foreign actors are targeting our election infrastructure in an attempt to undermine confidence in our democratic institutions. On a regular, almost daily basis, we learned more about the nature of and motives behind this new and dangerous development. Even as we received testimony from election administrators and experts from government, industry, and academia regarding the many issues faced in the conduct of elections, we were constantly reminded in news stories, by congressional hearings, and through reports from the intelligence community of the extraordinary threat from foreign actors using cyber weapons and social media to manipulate the electorate and to target our elections and cast doubt on the integrity of the elections process.

The current report makes numerous recommendations designed to harden our election infrastructure and safeguard its integrity and credibility.

We live in a nation that is unique in the tremendous importance it places on free speech. This remarkable privilege was enshrined in the First Amendment by the framers of the Constitution. Not only does the Constitution forbid official censorship, but it invests our government with the extraordinary responsibility of ensuring that all Americans can be heard. In this context, the ability of the citizenry to participate in elections and have their votes accurately cast and counted is paramount.

Over the course of this study, we were inspired by dedicated and enlightened election officials from across the nation and all levels of government. Such individuals are working tirelessly to improve accessibility, harness new technologies, and ensure the integrity of the results of elections. Unfortunately, these same officials often lack appropriate staff and resources and are routinely hampered in their work by a patchwork of laws and regulations that make it difficult to upgrade and modernize their election systems.

We also heard from researchers working to design better ballots, develop better and more secure voting systems, and identify new ways to quickly and reliably certify that the results of elections are reflective of the will of the voters. All too often, their efforts are underfunded, important research questions remain unaddressed, and there are challenges to translating research into practice.

The 2016 Presidential election was a watershed moment in the history of elections. The election exposed new technical and operational challenges that require the immediate attention of state and local governments, the federal government, researchers, and the American public. The election showed us that citizens must become more discerning consumers of information and that state and local governments must work collaboratively and together with the federal government to secure our election systems. Further, our leaders must speak candidly and apolitically about threats to our election systems. Transparent communication about threats to the integrity of our elections is vital. Openness is the most effective antidote to cynicism and distrust. In the interconnected world we increasingly live in, we want and need to hear what those beyond our borders think, but we must be cognizant of deliberate and deceitful efforts to spread disinformation and propaganda. The American people must have confidence that their leaders place the larger interests of democracy above all else. The future of voting is one in which a clear tension must be managed: we must prevent bad actors from corrupting our electoral process while delivering the means to provide suffrage to an electorate that is growing in size and complexity.

We are deeply indebted to the members of the committee for their dedication to our task and for the countless hours they spent exchanging ideas and reviewing testimony and background materials. Each member contributed thoughtfully and collegially to the committee's many discussions.

We are immensely grateful to the staff who worked tirelessly on behalf of the committee: Anne-Marie Mazza; Jon Eisenberg; Steven Kendall; Karolina Konarzewska; and consultant writer Bill Skane.

It has been our great pleasure and honor to lead this important study. We believe that the findings and recommendations laid out in this report provide the United States with a blueprint for an elections system that is accessible, reliable, verifiable, and secure.

Lee C. Bollinger and Michael A. McRobbie
Committee Co-chairs

Acknowledgments

ACKNOWLEDGMENT OF PRESENTERS

The committee gratefully acknowledges the thoughtful contributions of the following individuals who made presentations before the committee: Robert F. Bauer, Perkins Coie LLP; Brenda Bayes, State of Oregon; David Becker, Center for Election Innovation & Research; David Beirne, Federal Voting Assistance Program; Kenneth Bennett, Los Angeles County, CA; Matthew Blaze, University of Pennsylvania; Mary Brady, National Institute of Standards and Technology; Jonathan Brill, Scytl; Matthew Caulfied, University of Pennsylvania; Doug Chapin, University of Minnesota; Edgardo Cortes, State of Virginia Elections Board; McDermot Coutts, Unisyn Voting Solutions; David Fidler, Indiana University; Monica Flores, Los Angeles County, CA; Joe P. Gloria, Clark County, NV; Diane Cordry Golden, Association of Assistive Technology Act Programs; J. Alex Halderman, University of Michigan; Geoffrey Hale, U.S. Department of Homeland Security; Kathleen Hale, Auburn University; Hillary Hall, Boulder County, CO; Thad Hall, Fors Marsh Group; Shane Hamlin, Electronic Registration Information Center (ERIC); Jackie Harris, Democracy Live; General Michael Hayden, U.S. Air Force, National Security Agency, and Central Intelligence Agency (retired); Susan Hennessey, Brookings Institution; Douglas A. Kellner, State of New York; Merle King, Kennesaw State University; Joe Kiniry, Free & Fair; Robert Kolasky, U.S. Department of Homeland Security; Connie Lawson, State of Indiana and National Association of Secretaries of State; Matthew Masterson, U.S. Election Assistance Commission; Tim Mattice, The Election Center; Neal McBurnett, Free & Fair; Amber McReynolds, City and County of Denver, CO; Jennifer Morrell, Arapahoe County, CO; Jessica Myers, U.S. Election Assistance Commission; Brian Newby, U.S. Election Assistance Commission; Lawrence Norden, Brennan Center for Justice at New York University; Alex Padilla, National Association of Secretaries of State; Eddie Perez, Hart InterCivic; Whitney Quesenbery, Center for Civic Design; Peggy Reeves, State of Connecticut; Leslie Reynolds, National Association of Secretaries of State; Robert Rock, State of Rhode Island; Hilary Rudy, State of Colorado; John Schmitt, Five Cedars Group; Lisa Schur, Rutgers University; Alexander Schwarzmann, University of Connecticut; Will Senning, State of Vermont; James Simons, Everyone Counts; David Stafford, Escambia County (FL) Elections Office; Robert M. Stein, Rice University; and Anthony Stevens, State of New Hampshire.

ACKNOWLEDGMENT OF REVIEWERS

This Consensus Study Report was reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise. The purpose of this independent review is to provide candid and critical comments that will assist the National Academies of Sciences, Engineering, and Medicine in making each published report as sound as possible and to ensure that it meets the institutional standards for quality, objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process.

We thank the following individuals for their review of this report: Robert Bauer, Perkins Coie LLP; Matthew Blaze, University of Pennsylvania; Douglas Chapin, University of Minnesota; Judd Choate, Colorado Department of State; David Dill, Stanford University; Michael Haas, Wisconsin Election Commission; J. Alex Halderman, University of Michigan; Douglas Kellner, New York State Board of Elections; Philip Kortum, Rice University; Jane Lute, United Nations; Whitney Quesenbery, Center for Civic Design; Barbara Simons, IBM Corporation; David Stafford, Escambia County (FL) Elections Office; and Philip Stark, University of California, Berkeley.

Although the reviewers listed above provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations of this report nor did they see the final draft before its release. The review of this report was overseen by Anita K. Jones, University of Virginia and David C. Vladeck, Georgetown University Law Center. They were responsible for making certain that an independent examination of this report was carried out in accordance with the standards of the National Academies and that all review comments were carefully considered. Responsibility for the final content rests entirely with the authoring committee and the National Academies.

Contents

Appendixes

Boxes, Figures, and Tables

BOXES

FIGURES

TABLES

Summary

During the 2016 presidential election, America's election infrastructure was targeted by a foreign government.[1] According to assessments by members of the U.S. Intelligence Community,[2] actors sponsored by the Russian government "obtained and maintained access to elements of multiple US state or local electoral boards."[3] While the full

[1] For the purposes of this report, *election infrastructure* is defined as the physical and organizational structures and facilities and personnel needed for the operation of elections.

[2] The U.S. Intelligence Community consists of 16 agencies working under the coordination of the Office of the Director of National Intelligence. The 16 agencies are the: Central Intelligence Agency; Defense Intelligence Agency; Federal Bureau of Investigation; National Geospatial-Intelligence Agency; National Reconnaissance Office; National Security Agency/Central Security Service; U.S. Department of Energy; U.S. Department of Homeland Security (DHS); U.S. Department of State; U.S. Department of the Treasury; Drug Enforcement Administration; U.S. Air Force; U.S. Army; U.S. Coast Guard; U.S. Marine Corps; and U.S. Navy.

[3] The U.S. Department of Homeland Security (DHS) assessed **"that the types of systems Russian actors targeted or compromised were not involved in vote tallying."** See Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections, Intelligence Community Assessment," January 6, 2017, p. iii, available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf. Bolded text is original to the document.

By September 2017, voter registration systems or public election sites in 21 states had been identified by DHS as having been targeted by Russian hackers. See, e.g., National Association of Secretaries of State, "NASS Statement on US Department of Homeland Security (DHS) Outreach to 21 States Regarding Potential Targeting," September 25, 2017, available at: https://www.nass.org/node/284 and Horwitz, Sari, Ellen Nakashima, and Matea Gold, "DHS Tells States About Russian Hacking During 2016 Election," *Washington Post*, September 22, 2017.

Voter registration systems and public election websites (e.g., state "my voter" pages) are *election systems*. For the purposes of this report, election system is defined as a technology-based extent and impact of these activities is not known and our understanding of these events is evolving, there is little doubt that these efforts represented an assault on the American system of representative democracy.

The vulnerability of election infrastructure to cyberattacks became a growing concern during the campaign leading up to the 2016 presidential election, and in fall 2016, the federal government took the unusual step of issuing a joint statement from the U.S. Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI) urging state and local governments to be "vigilant and seek cybersecurity assistance from DHS."[4] In late December 2016, as the extent of Russian activities became apparent, President Barack Obama invoked sanctions against Russia for its efforts to disrupt the presidential election.[5] In early 2017, the nation's election systems were given critical infrastructure status.[6]

system that is used to collect, process, and store data related to elections and election administration. In addition to voter registration systems and public election websites, election systems include voting systems (the means through which voters cast their ballots), vote tabulation systems, election night reporting systems, and auditing systems.

Whether there were attacks on voting systems or vote tabulation systems is unknown. The committee authoring this report is not aware of an ongoing investigation into this possibility. In 2016, gaps in intelligence gathering, information sharing, and reporting led to problems that were underappreciated at the time of the intrusions leaving considerable uncertainty about what happened, even today. See, e.g., U.S. Senate Select Committee on Intelligence, "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations," May 8, 2018, pp. 1-2, available at: https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf.

[4] U.S. Department of Homeland Security and Office of the Director of National Intelligence, "Joint Statement from the Department of Homeland Security and the Office of the Director of National Intelligence on Election Security," October 7, 2016, available at: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

[5] In announcing the sanctions, the president stated, "Today, I have ordered a number of actions in response to the Russian government's aggressive harassment of U.S. officials and cyber operations aimed at the U.S. election. These actions follow repeated private and public warnings that we have issued to the Russian government, and are a necessary and appropriate response to efforts to harm U.S. interests in violation of established international norms of behavior." See The White House, Office of the Press Secretary, "Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment," December 29, 2016, available at: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity.

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

Critical infrastructure refers to "assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." See U.S. Department of Homeland Security, "What Is Critical Infrastructure?," available at: https://www.dhs.gov/what-critical-infrastructure.

Today, long-standing concerns about outdated and insecure voting systems and newer developments such as cyberattacks, the designation of election systems as critical infrastructure, and allegations of widespread voter fraud, have combined to focus attention on U.S. election systems and operations. The issues highlighted in 2016 add urgency to a careful reexamination of the conduct of elections in the United States and demonstrate a need to carefully consider tradeoffs with respect to access and cybersecurity. This report responds to the needs of this moment.

ELECTIONS IN THE UNITED STATES

Unlike other nations, the United States has no centralized, nationwide election authority. The Constitution leaves it to individual states to run and regulate elections, but Congress may make regulations that supersede state regulations on the conduct of federal contests.[7]

Motivated to make participation easier and election administration more efficient, some states have introduced new approaches to voting, such as in-person early voting, vote centers, and voting by mail. However, in an era when smart phones have become ubiquitous and the Internet plays an integral part in most people's lives, citizens must ask whether there are still further new innovative approaches to voting and consider what voting may look like in the future. Can, for example, safe and secure systems be developed to enable Internet or other remote voting in elections?

Efforts to Improve the Administration of Elections

Over the past two decades, numerous initiatives have been launched to improve U.S. election systems, with activity especially intense after the 2000 presidential election. Progress has been made since 2001, but old problems persist and new problems emerge. U.S. elections are subject to aging equipment, targeting by external actors, a lack of sustained funding, and growing expectations that voting should be more accessible, convenient, and secure. The present issues and threat environment provides an extraordinary opportunity to marshal science and technology to create more resilient and adaptive election systems that are accessible, reliable, verifiable, and secure.

Charge to the Committee

In 2016, amid concerns about the state of U.S. election infrastructure, the Carnegie Corporation of New York and the William and Flora Hewlett

[7] U.S. Constitution, Article I § 4.

Foundation provided support for the National Academies of Sciences, Engineering, and Medicine to consider the future of voting in the United States. In response, the National Academies appointed an ad hoc committee, the Committee on the Future of Voting: Accessible, Reliable, Verifiable Technology, to:

1. Document the current state of play in terms of technology, standards, and resources for voting technologies.
2. Examine challenges arising out of the 2016 federal election.
3. Evaluate advances in technology currently and soon-to-be available that can improve voting.
4. Offer recommendations that provide a vision of voting that is easier, accessible, reliable, and verifiable.

In carrying out its charge, the committee was mindful of the context in which its study was conducted. The committee saw its work as an opportunity to address concerns about the "hard" (e.g., all components of election systems including hardware and software) and "soft" (e.g., education and training of election workforce, law, and governance) issues associated with elections and to address new threats that could erode confidence in the results of elections. The committee recommendations articulated in this report address U.S. elections holistically, as the elections system itself is composed of numerous component systems. Issues related to voting (e.g., voter identification laws, gerrymandering, foreign and domestic disinformation, campaign financing, etc.) not addressed in this report were considered by the committee as outside its charge.

As this report illustrates, voting in the United States is a complicated process that involves multiple levels of government, personnel with a variety of skills and capabilities, and numerous electronic systems that interact in the performance of a multitude of tasks. Unfortunately, our current system is vulnerable to internal and external threats.

For this study, the committee examined the various election systems in use in the United States, the diverse parties involved in the administration of elections, research on elections, the availability of resources, and structural gaps. To create a system of voting for the future, the committee makes the following recommendations.[8]

[8] The initial digit in each numbered recommendation refers to the number of the chapter in this report in which the associated topic is discussed.

RECOMMENDATIONS ON COMPONENTS OF ELECTIONS

Voter Registration and Voter Registration Databases

Recommendations

4.1 Election administrators should routinely assess the integrity of voter registration databases and the integrity of voter registration databases connected to other applications. They should develop plans that detail security procedures for assessing voter registration database integrity and put in place systems that detect efforts to probe, tamper with, or interfere with voter registration systems. States should require election administrators to report any detected compromises or vulnerabilities in voter registration systems to the U.S. Department of Homeland Security, the U.S. Election Assistance Commission, and state officials.

4.2 Vendors should be required to report to their customers, the U.S. Department of Homeland Security, the U.S. Election Assistance Commission, and state officials any detected efforts to probe, tamper with, or interfere with voter registration systems.

4.3 All states should participate in a system of cross-state matching of voter registrations, such as the Electronic Registration Information Center (ERIC). States must ensure that, in the utilization of cross-matching voter databases, eligible voters are not removed from voter rolls.

4.4 Organizations engaged in managing and cross-matching voter information should continue to improve security and privacy practices. These organizations should be subject to external audits to ensure compliance with best security practices.

Voting by Mail, Including Absentee Voting

Recommendation

4.5 All voting jurisdictions should provide means for a voter to easily check whether a ballot sent by mail has been dispatched to him or her and, subsequently, whether his or her marked ballot has been received and accepted by the appropriate elections officials.

Pollbooks

Recommendations

4.6 Jurisdictions that use electronic pollbooks should have backup plans in place to provide access to current voter registration lists in the event of any disruption.

4.7 Congress should authorize and fund the National Institute of Standards and Technology, in consultation with the U.S. Election Assistance Commission, to develop security standards and verification and validation protocols for electronic pollbooks in addition to the standards and verification and validation protocols they have developed for voting systems.

4.8 Election administrators should routinely assess the security of electronic pollbooks against a range of threats such as threats to the integrity, confidentiality, or availability of pollbooks. They should develop plans that detail security procedures for assessing electronic pollbook integrity.

Ballot Design

Recommendation

4.9 State requirements for ballot design (inclusive of print, screen, audio, etc.) and testing should use best practices developed by the U.S. Election Assistance Commission and other organizations with expertise in voter usability design (such as the Center for Civic Design).

Voting Technology

Recommendations

4.10 States and local jurisdictions should have policies in place for routine replacement of election systems.

4.11 Elections should be conducted with human-readable paper ballots. These may be marked by hand or by machine (using a ballot-marking device); they may be counted by hand or by machine (using an optical scanner).[9] Recounts and audits should be conducted by human inspection of the human-readable por-

[9] A modern form of optical scanner, a *digital scanner,* captures, interprets, and stores a high-resolution image of the voter's ballot at a resolution of 300 dots per inch (DPI) or higher.

tion of the paper ballots. Voting machines that do not provide the capacity for independent auditing (e.g., machines that do not produce a voter-verifiable paper audit trail) should be removed from service as soon as possible.

4.12 Every effort should be made to use human-readable paper ballots in the 2018 federal election. All local, state, and federal elections should be conducted using human-readable paper ballots by the 2020 presidential election.

4.13 Computers and software used to prepare ballots (i.e., ballot-marking devices) should be separate from computers and software used to count and tabulate ballots (scanners). Voters should have an opportunity to review and confirm their selections before depositing the ballot for tabulation.[10]

Voting System Certification

Recommendations

4.14 If the principles and guidelines of the final Voluntary Voting System Guidelines are consistent with those proposed in September 2017, they should be adopted by the U.S. Election Assistance Commission.

4.15 Congress should:

a. authorize and fund the U.S. Election Assistance Commission to develop voluntary certification standards for voter registration databases, electronic pollbooks, chain-of-custody procedures, and auditing; and

b. provide the funding necessary to sustain the U.S. Election Assistance Commission's Voluntary Voting System Guidelines standard-setting process and certification program.

4.16 The U.S. Election Assistance Commission and the National Institute of Standards and Technology should continue the process of refining and improving the Voluntary Voting System Guidelines to reflect changes in how elections are administered, to respond to new challenges to election systems (e.g., cyberattacks), and to take advantage of opportunities as new technologies become available.

[10] Throughout this report, to be *counted* means to be included in a vote tally. *Tally* refers to the total number of votes cast. *Tabulation* refers to the aggregation of the votes cast by individual voters to produce vote totals.

4.17 Strong cybersecurity standards should be incorporated into the standards-setting and certification processes at the federal and state levels.

RECOMMENDATIONS ON ENSURING THE INTEGRITY OF ELECTIONS

Election Cybersecurity

Recommendations

5.1 Election systems should continue to be considered as U.S. Department of Homeland Security-designated critical infrastructure.

5.2 The U.S. Election Assistance Commission and U.S. Department of Homeland Security should continue to develop and maintain a detailed set of cybersecurity best practices for state and local election officials. Election system vendors and state and local election officials should incorporate these best practices into their operations.

5.3 The U.S. Election Assistance Commission should closely monitor the expenditure of funds made available to the states for election security through the 2018 omnibus appropriations bill to ensure that the funds enhance security practices and do not simply replace local dollars with federal support for ongoing activities.[11] The U.S. Election Assistance Commission should closely monitor any future federal funding designated to enhance election security.

5.4 Congress should provide funding for state and local governments to improve their cybersecurity capabilities on an ongoing basis.

Election Auditing

Recommendations

5.5 Each state should require a comprehensive system of post-election audits of processes and outcomes. These audits should be conducted by election officials in a transparent manner, with as much observation by the public as is feasible, up to limits imposed to ensure voter privacy.

5.6 Jurisdictions should conduct audits of voting technology and processes (for voter registration, ballot preparation, voting, election

[11] See H.R. 1625 - Consolidated Appropriations Act, 2018, Section 501, available at: https://www.congress.gov/bill/115th-congress/house-bill/1625/text.

reporting, etc.) after each election. Privacy-protected audit data should be made publicly available to permit others to replicate audit results.

5.7 Audits of election outcomes should include manual examination of statistically appropriate samples of paper ballots cast.

5.8 States should mandate risk-limiting audits prior to the certification of election results.[12] With current technology, this requires the use of paper ballots. States and local jurisdictions should implement risk-limiting audits within a decade. They should begin with pilot programs and work toward full implementation. Risk-limiting audits should be conducted for all federal and state election contests, and for local contests where feasible.

5.9 State and local jurisdictions purchasing election systems should ensure that the systems will support cost-effective risk-limiting audits.

5.10 State and local jurisdictions should conduct and assess pilots of end-to-end-verifiable election systems in elections using paper ballots.

Internet Voting

Recommendations

5.11 At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots.[13,14] Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.[15]

5.12 U.S. Election Assistance Commission standards and state laws should be revised to support pilot programs to explore and validate new election technologies and practices. Election officials are encouraged to seek expert and public comment on proposed new election technology before it is piloted.

[12] Risk-limiting audits examine individual randomly selected paper ballots until there is sufficient statistical assurance to demonstrate that the chance that an incorrect reported outcome escaping detection and correction is less than a predetermined risk limit.

[13] Inclusive of transmission via email or fax or via phone lines.

[14] The Internet is an acceptable medium for the transmission of unmarked ballots to voters so long as voter privacy is maintained and the integrity of the received ballot is protected.

[15] If secure Internet voting becomes feasible and is adopted, alternative ballot casting options should be made available to those individuals who do not have sufficient access to the Internet.

RECOMMENDATIONS ON SYSTEMIC ISSUES

Election Administrator and Poll Worker Training

Recommendations

6.1 Congress should provide adequate funding for the U.S. Election Assistance Commission to continue to serve as a national clearinghouse of information on election administration.

6.2 The U.S. Election Assistance Commission, with assistance from the national associations of state and local election administrators, should encourage, develop, and enhance information technology training programs to educate state and local technical staff on effective election administration.

6.3 Universities and community colleges should increase efforts to design curricula that address the growing organizational management and information technology needs of the election community.

The Voting Technology Marketplace

Recommendations

6.4 Congress should:
- a. create incentive programs for public-private partnerships to develop modern election technology;
- b. appropriate funds for distribution by the U.S. Election Assistance Commission for the ongoing modernization of election systems; and
- c. authorize and appropriate funds to the National Institute of Standards and Technology to establish Common Data Formats for auditing, voter registration, and other election systems.

6.5 Along with Congress, states should allocate funds for the modernization of election systems.

6.6 The U.S. Election Assistance Commission and the National Institute of Standards and Technology should continue to collaborate on changes to the certification process that encourage the modernization of voting systems.

6.7 The National Institute of Standards and Technology should complete the Common Data Format standard for election systems.

6.8 New election systems should conform to the Common Data Format standard developed by the National Institute of Standards and Technology.

The Federal Role

Recommendation

6.9 To improve the overall performance of the election process:

a. The president should nominate and Congress should confirm a full U.S. Election Assistance Commission and ensure that the U.S. Election Assistance Commission has sufficient members to sustain a quorum.

b. Congress should fully fund the U.S. Election Assistance Commission to carry out its existing functions.

c. Congress should require state and local election officials to provide the U.S. Election Assistance Commission with data on voting system failures during elections as well as information on other difficulties arising during elections (e.g., long lines, fraudulent voting, intrusions into voter registration databases, etc.). This information should be publicly available.

RECOMMENDATIONS ON SECURING THE FUTURE OF VOTING

7.1 Congress should provide appropriate funding to the U.S. Election Assistance Commission to carry out the functions assigned to it in the Help America Vote Act of 2002 as well as those articulated in this report.

7.2 Congress should authorize and provide appropriate funding to the National Institute of Standards and Technology to carry out its current elections-related functions and to perform the additional functions articulated in this report.

7.3 Congress should authorize and fund immediately a major initiative on voting that supports basic, applied, and translational research relevant to the administration, conduct, and performance of elections. This initiative should include academic centers to foster collaboration both across disciplines and with state and local election officials and industry.

The U.S. Election Assistance Commission, National Institute of Standards and Technology, U.S. Department of Homeland Security, National Science Foundation, and U.S. Department of Defense should sponsor research to:

- determine means for providing voters with the ability to easily check whether a ballot sent by mail has been dispatched to him or her and, subsequently, whether his or her marked ballot has been received and accepted by the appropriate elections officials;

- evaluate the reliability of various approaches (e.g., signature, biometric, etc.) to voter authentication;
- explore options for testing the usability and comprehensibility of ballot designs created within tight, pre-election timeframes;
- understand the effects of coercion, vote buying, theft, etc., especially among disadvantaged groups, on voting by mail and to devise technologies for reducing this threat;
- determine voter practices regarding the verification of ballot marking device–generated ballots and the likelihood that voters, both with and without disabilities, will recognize errors or omissions;
- assess the potential benefits and risks of Internet voting;
- evaluate end-to-end-verifiable election systems in various election scenarios and assess the potential utility of such systems for Internet voting; and
- address any other issues that arise concerning the integrity of U.S. elections.

CONCLUSION

As a nation, we have the capacity to build an elections system for the future, but doing so requires focused attention from citizens, federal, state, and local governments, election administrators, and innovators in academia and industry. It also requires a commitment of appropriate resources. Representative democracy only works if all eligible citizens can participate in elections, have their ballots accurately cast, counted, and tabulated, and be confident that their ballots have been accurately cast, counted, and tabulated.

1

Introduction

"The right to vote freely for the candidate of one's choice is of the essence of a democratic society . . ."[1]

"Every voter's vote is entitled to be counted once. It must be correctly counted and reported."[2]

During the 2016 presidential election, America's election infrastructure was targeted by a foreign government.[3] According to assessments by members of the U.S. Intelligence Community,[4] actors sponsored by the Russian government "obtained and maintained access to elements of multiple US state or local electoral boards."[5] While the full

[1] *Reynolds v. Sims*, 377 U.S. 533 (1964).

[2] *Gray v. Sanders*, 372 U.S. 368 (1963).

Throughout this report, to be *counted* means to be included in a vote tally. *Tally* refers to the total number of votes cast. *Tabulation* refers to the aggregation of the votes cast by individual voters to produce vote totals.

[3] For the purposes of this report, *election infrastructure* is defined as the physical and organizational structures and facilities and personnel needed for the operation of elections.

[4] The U.S. Intelligence Community consists of 16 agencies working under the coordination of the Office of the Director of National Intelligence. The 16 agencies are the: Central Intelligence Agency; Defense Intelligence Agency; Federal Bureau of Investigation; National Geospatial-Intelligence Agency; National Reconnaissance Office; National Security Agency/Central Security Service; U.S. Department of Energy; U.S. Department of Homeland Security (DHS); U.S. Department of State; U.S. Department of the Treasury; Drug Enforcement Administration; U.S. Air Force; U.S. Army; U.S. Coast Guard; U.S. Marine Corps; and U.S. Navy.

[5] The U.S. Department of Homeland Security (DHS) assessed **"that the types of systems Russian actors targeted or compromised were not involved in vote tallying."** See Office of the

extent and impact of these activities is not known and our understanding of these events is evolving, there is little doubt that these efforts represented an assault on the American system of representative democracy. The 2016 Russian probes of the U.S. voting infrastructure also were accompanied by directed social media campaigns spreading disinformation that sought to divide the American electorate and undermine confidence in democratic institutions. As former Central Intelligence Agency and National Security Agency Director Michael Hayden observed in testimony to the committee that authored this report, these efforts represented part of a sustained campaign to discredit Western countries and institutions and specifically "Western democratic processes and the American election."[6] The Russian campaign represents an unsettling development that adds greatly to the technical and operational challenges facing election administrators.

The vulnerability of election systems to cyberattacks became a growing concern during the campaign leading up to the 2016 presidential election.[7] That threat caused so much concern that, in the fall of 2016, the federal

Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections, Intelligence Community Assessment," January 6, 2017, p. iii, available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf. Bolded text is original to the document.

By September 2017, voter registration systems or public election sites in 21 states had been identified by DHS as having been targeted by Russian hackers. See, e.g., National Association of Secretaries of State, "NASS Statement on US Department of Homeland Security (DHS) Outreach to 21 States Regarding Potential Targeting," September 25, 2017, available at: https://www.nass.org/node/284 and Horwitz, Sari, Ellen Nakashima, and Matea Gold, "DHS Tells States About Russian Hacking During 2016 Election," *Washington Post*, September 22, 2017.

Voter registration systems and public election websites (e.g., state "my voter" pages) are *election systems*. For the purposes of this report, election system is defined as a technology-based system that is used to collect, process, and store data related to elections and election administration. In addition to voter registration systems and public election websites, election systems include voting systems (the means through which voters cast their ballots), vote tabulation systems, election night reporting systems, and auditing systems.

Whether there were attacks on voting systems or vote tabulation systems is unknown. The committee authoring this report is not aware of an ongoing investigation into this possibility. In 2016, gaps in intelligence gathering, information sharing, and reporting led to problems that were underappreciated at the time of the intrusions leaving considerable uncertainty about what happened, even today. See, e.g., U.S. Senate Select Committee on Intelligence, "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations," May 8, 2018, pp. 1-2, available at: https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf.

[6] Comments by General Michael Hayden at the third meeting of the Committee on the Future of Voting, the National Academies, October 18, 2017, Washington, DC, webcast available at: https://livestream.com/accounts/7036396/events/7752647.

[7] By late fall 2016, the U.S. intelligence community had determined that Russia had directed the theft and disclosure of emails from U.S. persons and institutions, including U.S. political organizations, for the purpose of "interfer[ing] with the US election process." See U.S. Department of Homeland Security and Office of the Director of National Intelligence, "Joint Statement from the Department of Homeland Security and the Office of the Director of National Intelligence

government took the unusual step of issuing a joint statement from the U.S. Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI) urging state and local governments to be "vigilant and seek cybersecurity assistance from DHS."[8] In late December 2016, as the extent of Russian activities became apparent, President Barack Obama invoked sanctions against Russia for its efforts to disrupt the presidential election. In early January 2017, then-DHS Secretary Jeh Johnson observed that, "Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law." In early 2017, the nation's election systems were given critical infrastructure status.[9]

Since the 2000 election, election infrastructure has been a focus of attention due to concerns about aging and insecure voting equipment, inadequate poll worker training, insufficient numbers of voting machines and pollbooks, deficient voter registration information systems, and inadequate verification procedures for votes cast. Long before concerns about Russian interference surfaced, state and local election administrators had been forced to reevaluate and modernize the operation of voting systems[10] in the wake of incidents such as the "hanging chad" debacle in the 2000 presidential election and long lines that occurred in some jurisdictions in the 2004, 2008, and 2012 elections. In advance of the 2016 election, as they had in the past, officials worked aggressively to ensure that the 2016 national election would run smoothly and without disruptions and that election systems—including public election websites, voter registration systems, voting systems, vote tabulation systems, election night reporting systems, and auditing systems—would meet the challenges of a national election.

Today, long-standing concerns about outdated and insecure voting systems and newer developments such as cyberattacks, the designation of election systems as critical infrastructure, and allegations of widespread voter fraud, have combined to focus attention on U.S. election systems

on Election Security," October 7, 2016, available at: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

[8] "Joint Statement from the Department of Homeland Security and the Office of the Director of National Intelligence on Election Security."

Critical infrastructure refers to "assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." See U.S. Department of Homeland Security, "What Is Critical Infrastructure?," available at: https://www.dhs.gov/what-critical-infrastructure.

[9] Johnson, Jeh, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," January 6, 2017, available at: https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

[10] Throughout this report, the term *voting system* refers to the means through which voters cast their ballots.

and operations. The issues highlighted in 2016 add urgency to a careful reexamination of the conduct of elections in the United States and demonstrate a need to carefully consider tradeoffs with respect to access and cybersecurity. This report responds to the needs of this moment.

ELECTIONS IN THE UNITED STATES

Unlike other nations, the United States has no centralized, nationwide election authority.[11] The Constitution leaves it to individual states to run and regulate elections (see Box 1-1).[12] Congress may, however, make regulations that supersede state regulations on the conduct of federal contests. Federal anti-discrimination laws have been enacted to ensure registration and poll access for all eligible voters.[13]

Until the Australian (secret) ballot was adopted by most of the states in the 1890s, many Americans voted in public, sometimes casting their votes orally, with no voting booths or other means of protecting the confidentiality of an individual's vote.[14] (See Figure 1-1.)

[11] Decentralization allows voting technologies to be adapted to meet local needs, laws, and traditions. It may spur innovation, with states serving as, in the words of U.S. Supreme Court Justice Louis Brandeis, "laboratories of democracy." Decentralization may also help impede certain attacks on election infrastructure, as it greatly multiplies potential points of attack.

Decentralization implies, however, that there will be a diversity of strength and weakness, and malicious actors have the freedom to focus on the most weakly defended systems. In a close election, successful attacks against a few weakly protected swing states or swing districts could tip national results. Moreover, a successful attack anywhere will detract from voter confidence everywhere.

States and localities often lack the resources that a central government might bring to support of election infrastructure.

Decentralization also fragments the markets for election technologies. This might affect costs and hinder innovation.

The diffuse responsibility for American elections can also contribute to a lack of clarity with regard to the level of government that is responsible for responding to acute attacks on election infrastructure.

[12] In some states and jurisdictions, the conduct of elections and the registration of voters are administered by two separate and distinct entities.

[13] See U.S. Constitution, Article I § 4 and 4th, 15th, 19th, 24th, and 26th Amendments to the U.S. Constitution; Voting Rights Act, 52 U.S.C. §§ 10101 *et seq.*; Voting Age Act, 52 U.S.C. §§ 10701 and 10702; Voting Accessibility for Elderly and Handicapped Act, 52 U.S.C. §§ 20101 *et seq.*; Uniformed and Overseas Citizens Absentee Voting Act, 52 U.S.C. §§ 20301 *et seq.*; and National Voter Registration Act, 52 U.S.C. §§ 20501 *et seq.*

[14] See Ludington, Arthur C., *American Ballot Laws, 1888–1910.* New York State Education Department Bulletin No. 448 (Albany: University of the State of New York, 1911); Evans, Eldon Cobb, *A History of the Australian Ballot System in the United States* (Chicago: University of Chicago Press, 1917); and Katz, Jonathan N. and Brian R. Sala, "Careerism, Committee Assignments, and the Electoral Connection," *American Political Science Review*, 1996, No. 90, pp. 21-33, Table 1.

BOX 1-1 Election Management and the U.S. Constitution

The U.S. Constitution as originally ratified is silent about who can vote. Suffrage requirements were left to the states, which until 1828 generally restricted voting to white male property owners. The Constitution grants Congress the authority to make regulations that supersede state laws and regulations pertaining to congressional elections.

Over time, by law and custom, each state has devised and periodically revised its own election procedures. Many procedures are reflected in local laws. Every state has a chief election official who has oversight responsibility for elections in the state. For about half of the states, this is an elected secretary of state. Other states have other leadership models (e.g., appointed secretaries of state, lieutenant governors, and election boards).

The particular voting systems used to cast ballots are chosen independently by the states, often by local governments. The federal government, through the Election Assistance Commission, helps to develop standards that guide the development of voting systems, but these standards are voluntary—states are free to adopt or ignore them. Decisions regarding the design of (and support for) other election systems are likewise the prerogative of the individual states.

Today, U.S. elections are administered by thousands of jurisdictions. Elections encompass both highly visible contests, such as the presidential election, and contests to elect minor local officials. Some jurisdictions contain fewer than 100 voters while others contain millions. Elections are overseen by state and/or local officials acting according to laws and rules promulgated by state and local governments. Many elections offices have few dedicated staff and little access to the latest information technology (IT) training or tools.[15] While elections end for most voters once they have cast their ballots and the results of the election are announced, election administrators must constantly be planning for future elections.

Motivated to make participation easier and election administration more efficient, some states have introduced new modes of voting, such as in-person early voting, vote centers, and voting by mail. Estimates are difficult to make with available data, but in the 2016 presidential election, it appears that between 55 and 60 million of 138.8 million of those who

[15] Kimball, David C., and Brady Baybeck, "Are All Jurisdictions Equal? Size Disparity in Election Administration," *Election Law Journal*, 2013, No. 12, pp. 130-145.

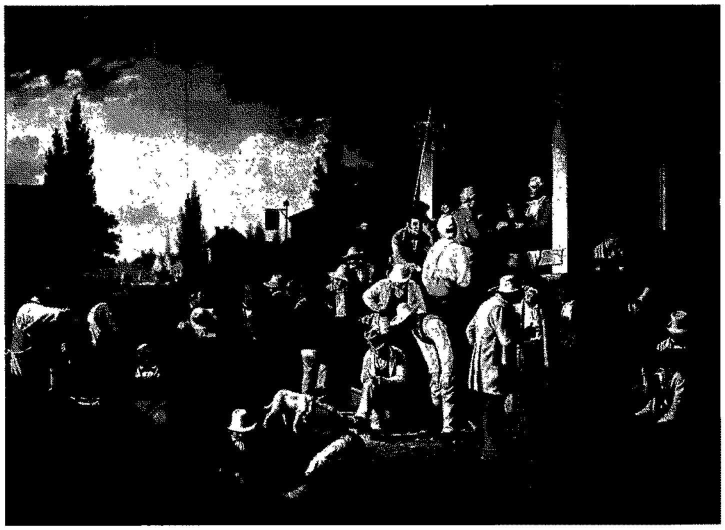


FIGURE 1-1 George Caleb Bingham, American, 1811–1879; *The County Election*, 1852; oil on canvas; 38 x 52 inches; Saint Louis Art Museum, Gift of Bank of America 44:2001. Image courtesy Saint Louis Art Museum.
Bingham's painting depicts the chaotic and public nature of voting in the 19th century. Voters often approached an election official to vote by voice while politicians stood close by to watch and influence voters. Nearby, sometimes libations awaited those who had cast the "right vote."

voted took advantage of these emerging approaches.[16] However, in an era when smart phones have become ubiquitous and the Internet plays an integral part in most people's lives, citizens must ask whether there are still further new innovative approaches to voting and consider what voting may look like in the future. Can, for example, safe and secure systems be developed to enable Internet or other remote voting in elections?

[16] Estimates of the number of voters who used various voting modes are imprecise because states do not uniformly report turnout by voting mode. These estimates are derived from two sources, respectively: U.S. Census Bureau, "Current Population Survey, Voting and Registration Supplement," 2016 and U.S. Election Assistance Commission, "2016 Election Administration and Voting Survey" (EAVS), June 29, 2016.

EFFORTS TO IMPROVE THE ADMINISTRATION OF ELECTIONS

Over the past two decades, numerous initiatives have been launched to improve U.S. election systems, with activity especially intense after the 2000 presidential election. Two national bipartisan commissions, the National Commission on Federal Election Reform and the Commission on Federal Election Reform, followed a long-standing tradition of assembling panels of notable politicians, academics, and public intellectuals to study national crises and propose reforms. The National Commission on Federal Election Reform, which conducted its work in 2001, was chaired by former Presidents Gerald Ford and Jimmy Carter.[17] The report of the Ford-Carter Commission, titled "To Assure Pride and Confidence in the Electoral Process," issued several recommendations concerning voter registration, election systems, and election operations. These recommendations informed the Help America Vote Act (HAVA) (see below) passed in 2002.[18,19] The Commission on Federal Election Reform, chaired by President Carter and former-Secretary of State James Baker, conducted its work from 2004 to 2005. Its report, "Building Confidence in U.S. Elections," looked beyond HAVA to provide recommendations related to voter registration, voter identification, improved security for elections (including voter-verifiable paper trails), and independent, professional election administration.[20]

Universities have contributed to sustained efforts to build a research-based infrastructure aimed at improving the administration of elections on a scientific and technical basis. Noting a "distressing lack of previous research" on voting that had led to the use of technologies that were "unreliable and inaccurate," the Caltech/MIT Voting Technology Project (VTP) was established in December 2000 to develop voting systems standards and testing practices on a foundation of scientific and engineering research. Over time, VTP has created a body of research and facilitated new collaborations with state and local election administrators to improve voting systems and the voting experience.[21] Other current university-based programs include the Center for Voting Technology Research at the Univer-

[17] See https://millercenter.org/issues-policy/governance/the-national-commission-on-federal-election-reform.

[18] The National Commission on Federal Election Reform, "To Assure Pride and Confidence in the Electoral Process," 2001, available at: http://web1.millercenter.org/commissions/comm_2001.pdf.

[19] Help America Vote Act of 2002 (Pub.L. 107–252).

[20] Commission on Federal Election Reform, "Building Confidence in U.S. Elections," 2005, available at: https://www.eac.gov/assets/1/6/Exhibit%20M.PDF.

[21] See https://vote.caltech.edu.

sity of Connecticut[22] and the Voting System Technical Oversight Program at Ball State University.[23]

HAVA created the U.S. Election Assistance Commission (EAC), an independent bipartisan federal agency, to serve as a clearinghouse for election administration research and information and to disburse federal funds to states for the replacement of antiquated voting systems and the improvement of election administration; mandated that states create centralized, computerized voting registration systems; and required minimal standards for federal elections.[24] In order to facilitate the modernization of election technologies, HAVA authorized a $3 billion appropriation for the purchase of new voting systems. HAVA also gave the National Institute for Standards and Technology (NIST) a key role in improving election infrastructure through, for example, the development of voluntary voting system guidelines.

In March 2013, the bipartisan Presidential Commission on Election Administration was established by President Obama to

> identify best practices and otherwise make recommendations to promote the efficient administration of elections in order to ensure that all eligible voters have the opportunity to cast their ballots without undue delay, and to improve the experience of voters facing other obstacles in casting their ballots, such as members of the military, overseas voters, voters with disabilities, and voters with limited English proficiency.[25]

The commission's resulting report, "The American Voting Experience," warned of a new "impending crisis in voting technology" as the voting

[22] See https://voter.engr.uconn.edu/voter/.

[23] See http://bowencenterforpublicaffairs.org/institutes/policy-research/election-admin/vstop.

[24] The EAC's "four commissioners are nominated by the President on recommendations from the majority and minority leadership in the U.S. House of Representatives and the U.S. Senate. No more than two commissioners may belong to the same political party. Once confirmed by the full Senate, commissioners may serve two consecutive terms." See U.S. Election Assistance Commission, "About U.S. EAC: Commissioners," available at: https://www.eac.gov/about/commissioners/.

There are currently two vacancies on the commission. Any action of the commission authorized by HAVA requires approval of at least three of its members. See HAVA 42 U.S.C. § 15328.

[25] The White House, "Executive Order – Establishment of the Presidential Commission on Election Administration," March 23, 2013, available at: https://obamawhitehouse.archives.gov/the-press-office/2013/03/28/executive-order-establishment-presidential-commission-election-administr.

systems developed and installed in the early 2000s began to wear out and fail. [26]

At the state level, election administrators have been collaborating with academic researchers, NIST,[27] and the EAC on experiments to improve ballot design; improve polling place accessibility; develop language assistance resources; expand the use of voting by mail; operate vote centers; improve voter experience in polling places; and conduct audits to test the security of voting systems.

While progress has been made since 2001, old problems persist and new problems emerge. U.S. elections are subject to aging equipment, targeting by external actors, a lack of sustained funding, and growing expectations that voting should be more accessible, convenient, and secure. The present issues and threat environment provide an extraordinary opportunity to marshal science and technology to create more resilient and adaptive election systems that are accessible, reliable, verifiable, and secure.

CHARGE TO THE COMMITTEE

In 2016, amid concerns about the state of U.S. election infrastructure, the Carnegie Corporation of New York and the William and Flora Hewlett Foundation provided support for the National Academies of Sciences, Engineering, and Medicine to consider the future of the voting in the United States. In response, the National Academies appointed an ad hoc committee, the Committee on the Future of Voting: Accessible, Reliable, Verifiable Technology, to:

1. Document the current state of play in terms of technology, standards, and resources for voting technologies.
2. Examine challenges arising out of the 2016 federal election.
3. Evaluate advances in technology currently and soon-to-be available that can improve voting.
4. Offer recommendations that provide a vision of voting that is easier, accessible, reliable, and verifiable.

In carrying out its charge, the committee was mindful of the context in

[26] Presidential Commission on Election Administration, "The American Voting Experience: Report and Recommendations of the Presidential Commission on Election Administration," January 2014, available at: https://www.eac.gov/assets/1/6/Amer-Voting-Exper-final-draft-01-09-14-508.pdf, p. 4.

The report offered recommendations to address this "impending crisis" but also voter registration, access to the polls, and polling place management.

[27] NIST often carries out its work in collaboration with researchers, election administrators, vendors, and the U.S. Election Assistance Commission.

which its study was conducted. The committee saw its work as an opportunity to address concerns about the "hard" (e.g., all components of election systems including hardware and software) and "soft" (e.g., education and training of election workforce, law, and governance) issues associated with elections and to address new threats that could erode confidence in the results of elections. The committee recommendations articulated in Chapters 4, 5, 6, and 7 address U.S. elections holistically, as the elections system is compromised of numerous component systems. Issues related to voting (e.g., voter identification laws, gerrymandering, foreign and domestic disinformation, campaign financing, etc.) not addressed in this report were considered by the committee as outside its charge.

Over the course of this study, the committee reviewed extensive background materials. It held six meetings where invited experts spoke to the committee about a range of topics including voter registration, voting accessibility, voting technologies and market impediments to technological innovation, cybersecurity, post-election audits, and the education and training of election workers. Agendas for the committee's meetings appear in Appendix B. The committee did not access classified information but instead relied on information in the public domain, including state and federal government reports, published academic literature, testimony from congressional hearings, and presentations to the committee.

ORGANIZATION OF THE REPORT

Chapter 2 provides an overview of issues arising in the 2016 election. Chapter 3 provides an overview of U.S. election systems. Chapters 4, 5, and 6 describe challenges for election administration and provide the committee's findings and recommendations. Chapter 7 offers the committee's conclusions about securing the future of voting and offers concluding recommendations.

2

Voting and the 2016 Presidential Election

Federal elections are an enormous undertaking. There are thousands of election administration jurisdictions in the United States, and in the 2016 presidential election, there were 178,217 individual precincts[1] and 116,990 physical Election Day polling places.[2,3] Election administration jurisdictions operated more than 8,500 locations where ballots could be cast prior to Election Day.[4]

Greater than 60 percent of the U.S. voting-eligible population (138.8 million voters out of 230.6 million eligible Americans) cast ballots in the 2016 presidential election.[5] Voter turnout exceeded 70 percent in four

[1] An individual precinct is a geographic voting area to which individuals are assigned and that determine the ballot type voters receive.

[2] A polling place is the location where one can vote on Election Day.

[3] "2016 Election Administration and Voting Survey" (EAVS), p.13.

Statistics quoted in this report that rely on the EAVS reflect answers from jurisdictions that provided information to the EAC and totals, therefore, may not add up to 100 percent. The EAVS contains the most comprehensive nationwide data about election administration in the United States. It includes responses from all 50 states, the District of Columbia, and four U.S. territories. The U.S. Election Assistance Commission (EAC) administers the survey to meet its obligations under the Help America Vote Act of 2002 to serve as a national clearinghouse and resource for the compilation of information related to federal elections. Data are collected at the local level by counties or the county equivalent and include information related to voter registration; military and overseas voters; early and by mail voting; provisional voting; voter participation; voting equipment usage; and poll workers, polling places, and precincts.

[4] Ibid.

[5] See United States Election Project, "2016 November General Election Turnout Rates," available at: http://www.electproject.org/2016g.

states.[6] Greater than 41 percent of all ballots were cast before Election Day; of these, approximately 17 percent were cast using in-person early voting while nearly 24 percent were cast by mail.[7] While rates of voting by mail vary significantly across the country, nationally approximately 80 percent of ballots transmitted to voters were returned. In most states, greater than 90 percent of returned ballots met eligibility requirements and were counted.[8]

ISSUES ARISING IN THE 2016 PRESIDENTIAL ELECTION

During the 2016 election, the media and citizen groups who monitor the voting process reported problems experienced at the polls, such as confusion over state requirements regarding voter identification, difficulties with polling place procedures, and faulty voting equipment. However, in responses to the "Survey of the Performance of the American Electorate," the only large-scale academic survey devoted to election administration topics, the vast majority of voters reported that they did not encounter problems at the polls or when voting by mail.[9] This does not mean that there were not problems that occurred unbeknownst to the voter. If an electronic voting machine, for example, were to change a vote after a voter had completed the voting process, the voter would be unaware of the problem and have no reason to report dissatisfaction.

In general, responses to the survey were similar to those given following the 2008 and 2012 elections. The only common problem reported in 2016 was long lines in some locations. However, the average wait times reported in 2016 were significantly less than those reported in 2012, when the issue was elevated to national prominence.

The 2016 election was distinguished by two notable developments: (1) the targeting of many states' voter registration systems and public election websites by Russian actors; and (2) assertions by the new president that millions of individuals voted illegally. In addition, the Russian government made efforts to influence the outcome of the election through a disinformation campaign using social media and other tactics (see Appendix C).

[6] Ibid. The four states were Colorado, Maine, Minnesota, and New Hampshire.

[7] Ibid, p. 8.

[8] Ibid, p. i.

[9] Stewart, Charles III. "2016 Survey of the Performance of American Elections: Final Report," 2017, available at: http://dx.doi.org/10.7910/DVN/Y38VIQ. Dr. Stewart is a member of the committee that authored the current report.

Foreign Targeting of Election Systems

In the summer of 2016, as election administrators were preparing for the upcoming presidential election, they were notified by then-Secretary of the U.S. Department of Homeland Security (DHS) Jeh Johnson of growing evidence of foreign intrusions into state election systems and of the possibility of foreign interference. In June, federal cybersecurity experts noticed that the network credentials of an Arizona county elections worker, which would allow access to Arizona's state voter registration system, had been posted on a site frequented by suspected Russian hackers. Several weeks later, Illinois Board of Elections' information technology staff noticed a significant increase in activity involving their voter registration system: "Malicious queries were hitting [...the voter registration system] 5 times per second, 24 hours a day, looking for a way to break in."[10] Illinois officials took the website offline and discovered that the attack had originated overseas and had begun weeks earlier.

In October 2016, DHS and the Office of the Director of National Intelligence (ODNI) issued a joint statement on election security. The statement said that some states had seen scanning and probing of their election systems, "which in most cases originated from servers operated by a Russian company."[11] DHS urged election administrators to remain vigilant.

By late December 2016, the federal government, through a Joint Analysis Report, provided further details about Russian cyber-attacks that had targeted one of the political party's campaigns.[12] In response, President Obama expelled 35 Russian diplomats from the United States and imposed sanctions on two Russian intelligence services. The president declared that, "All Americans should be alarmed by Russia's actions," and said that his actions were "a necessary and appropriate response to efforts to harm U.S. interests in violation of established international norms of behavior."[13]

In January 2017, ODNI issued a report, "Assessing Russian Activities and Intentions in Recent US Elections." The report documented Russia's use of cyber tools and media campaigns to influence the 2016 U.S. presidential

[10] Fessler, Pam, "Timeline: Foreign Efforts to Hack State Election Systems and How Officials Responded," National Public Radio, July 31, 2017.

[11] "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security."

[12] U.S. Department of Homeland Security and Federal Bureau of Investigation, "GRIZZLY STEPPE – Russian Malicious Cyber Activity," Joint Analysis Report JAR-16-20296A, December 29, 2016, available at: https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

[13] The White House. Office of the Press Secretary, "Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment," December 29, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity.

election. Although the report primarily covered influence operations aimed at the political campaigns, it also addressed efforts to gain access to technologies associated with administering elections. It stated that:

> Russian intelligence obtained and maintained access to elements of multiple US state or local electoral boards. **DHS assesses that the types of systems Russian actors targeted or compromised were not involved in vote tallying. . . . We assess Moscow will apply lessons learned from its Putin-ordered campaign aimed at the US presidential election to future influence efforts worldwide, including against US allies and their election processes.**[14]

In early January 2017 Secretary Johnson designated the nation's election infrastructure as a subsector of the nation's critical infrastructure, stating,

> I have determined that election infrastructure in this country should be designated as a subsector of the existing Government Facilities critical infrastructure sector. Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law.
>
> I have reached this determination so that election infrastructure will, on a more formal and enduring basis, be a priority for cybersecurity assistance and protections that the Department of Homeland Security provides to a range of private and public sector entities. By "election infrastructure," we mean storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments." [15]

By September 2017, voter registration systems or public election sites in 21 states had been identified by DHS as having been targeted by Russian hackers.[16] In May 2018, the U.S. Senate Select Committee on Intelligence released a summary of its initial findings and recommendations regarding

[14] Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections, Intelligence Community Assessment," January 6, 2017, p. iii, available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf. Bolded text is original to the document. This declassified assessment is based on a "highly classified assessment," but its conclusions are "identical to the highly classified assessment" (see p. i).

[15] See https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

[16] Horwitz, Sari, Ellen Nakasmina, and Matea Gold, "DHS Tells States About Russian Hacking During 2016 Election," *Washington Post*, September 22, 2017.

the Russian targeting of election infrastructure during the 2016 election. The report states

- "In at least six states, the Russian-affiliated cyber actors went beyond scanning and conducted malicious access attempts on voting-related websites. In a small number of states, Russian-affiliated cyber actors were able to gain access to restricted elements of election infrastructure. In a small number of states, these cyber actors were in a position to, at a minimum, alter or delete voter registration data; however, they did not appear to be in a position to manipulate individual votes or aggregate vote totals." [17]
- "In addition to the cyber activity directed at state election infrastructure, Russia undertook a wide variety of intelligence-related activities targeting the U.S. voting process. These activities began at least as early as 2014, continued through Election Day 2016, and included traditional information gathering efforts as well as operations likely aimed at preparing to discredit the integrity of the U.S. voting process and election results."[18]

Assertion of Illegal Voting During the 2016 Election

Donald J. Trump won the presidency in 2016, having received a majority of electoral votes.[19,20] He did not win the popular vote, but claimed in late November 2016 that he would have won the popular vote "if you deduct the millions of people who voted illegally."[21] He repeated this claim in a January 2017 meeting with Congressional leaders, asserting that between 3 and 5 million illegal immigrants voted for Hillary Clinton.[22]

In response to the president's assertion, the bipartisan National Association of Secretaries of State (NASS) issued the following statement:

> We are not aware of any evidence that supports the voter fraud claims

[17] U.S. Senate Select Committee on Intelligence, "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations," May 8, 2018, pp. 1-2, available at: https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf.

[18] Ibid, p. 2.

[19] United States Congress, *Congressional Record,* Jan. 6, 2017, p. H190.

[20] President Trump received nearly 2.9 million fewer popular votes than his principal opponent, Hillary R. Clinton. Trump received 62,984,825 votes, compared to 65,863,516 for Clinton. See U.S. Federal Election Commission, "Official 2016 Presidential General Election Results," January 30, 2017, available at: https://transition.fec.gov/pubrec/fe2016/2016presgeresults.pdf.

[21] Trump, Donald, Twitter Post, November 27, 2016, 3:30 p.m., available at: https://twitter.com/realdonaldtrump/status/802972944532209664?lang=en.

[22] Shear, Michael D. and Emmarie Huetteman, "Trump Repeats Lie About Popular Vote in Meeting with Lawmakers," *New York Times*, January 23, 2017.

> made by President Trump, but we are open to learning more about the Administration's concerns. In the lead up to the November 2016 election, secretaries of state expressed their confidence in the systemic integrity of our election process as a bipartisan group, and they stand behind that statement today.[23]

The committee authoring the current study did not find evidence of large-scale illegal voting in the 2016 election.

On May 11, 2017, President Trump established the Presidential Advisory Commission on Election Integrity. Vice President Mike Pence was appointed chair of the commission, and Kansas Secretary of State Kris Kobach was appointed as vice chair. The commission was asked to

> study vulnerabilities in voting systems used for federal elections that could lead to improper voter registrations, improper voting, fraudulent voter registrations, and fraudulent voting. The Commission will also study concerns about voter suppression, as well as other voting irregularities. The Commission will utilize all available data, including state and federal databases.[24]

On January 3, 2018, after two meetings of the commission, President Trump announced its disbanding.[25] The commission had been embroiled in numerous controversies, including a request for voter registration files that both Republican and Democratic state officials considered overly broad[26] and questions about whether commission proceedings complied with the Federal Advisory Committee Act and whether its own members had been excluded from deliberations.[27] The commission did not issue any reports before it was disbanded.

President Trump subsequently asked DHS to review the issue of voter fraud. When asked if DHS had plans to pursue the fraud issues, DHS spokesperson Tyler Houlton stated that the department "continues to work in support of state governments who are responsible for administering elec-

[23] National Association of Secretaries of State, "Jan. 24. Statement by NASS," January 24, 2017, available at: http://www.nass.org/index.php/news-releases-and-statements/release-nass-statement-election-integrity-jan17/.

[24] See https://www.whitehouse.gov/the-press-office/2017/05/11/president-announces-formation-bipartisan-presidential-commission.

[25] See https://www.whitehouse.gov/presidential-actions/executive-order-termination-presidential-advisory-commission-election-integrity/.

[26] Wines, Michael, "Asked for Voters' Data, States Give Trump Panel a Bipartisan 'No'," *New York Times,* July 1, 2017.

[27] Wines, Michael and Maggie Haberman, "Trump Closes Voter Fraud Panel That Bickered More Than It Revealed," *New York Times,* January 5, 2018.

tions, with efforts focused on securing elections against those who seek to undermine the election system or its integrity."[28]

CONCLUSION

As in previous federal elections, election administrators oversaw a complex voting process during the 2016 presidential election. Efforts by the Russian government to probe systems that help administer elections, along with related efforts to influence the election using the Internet, prompted a new awareness of additional potential vulnerabilities. The DHS designation of election infrastructure as critical national infrastructure adds an additional facet into the election process. The following chapters describe U.S. election systems and consider how developments in 2016 and 2017 and issues already associated with election infrastructure may be addressed to make voting in the future more accessible, reliable, verifiable, and secure.

[28] Volz, Dustin and Julia Harte, "DHS Election Unit Has No Plans for Probing U.S. Voter Fraud-Sources," *Reuters*, January 5, 2018.

3

Voting in the United States

In the United States, federal elections occur every 2 years in even-numbered years.[1] Federal regulation of elections is limited, most importantly governing voting rights and campaign finance and affecting when elections for Congress are held. The major aspects of election administration are determined by state and local laws, and elections are overseen by state and local administrators. Although local control over elections leads to variations in specific processes, elections follow the same general process throughout the country (see Figure 3-1).

During each federal election, all 435 members of the House of Representatives are elected for 2-year terms. Senators are elected for staggered 6-year terms. This means that roughly one-third of the Senate is elected every 2 years. Presidential elections are held concurrently with House and Senate elections every fourth year.

State and local contests, including ballot initiatives and referenda, often appear on the ballot alongside federal contests in even-numbered years. However, a few states hold state elections in odd-numbered years, [2] and it is common for local governments to hold elections in the spring, rather than in the fall.

Elections for most offices have a preliminary race wherein the initial field of candidates is winnowed to a smaller number. Most commonly,

[1] Special elections for members of Congress may be held to fill vacancies in both even and odd years.

[2] Five states, Kentucky, Louisiana, Mississippi, New Jersey, and Virginia, hold major state elections in odd-numbered years.

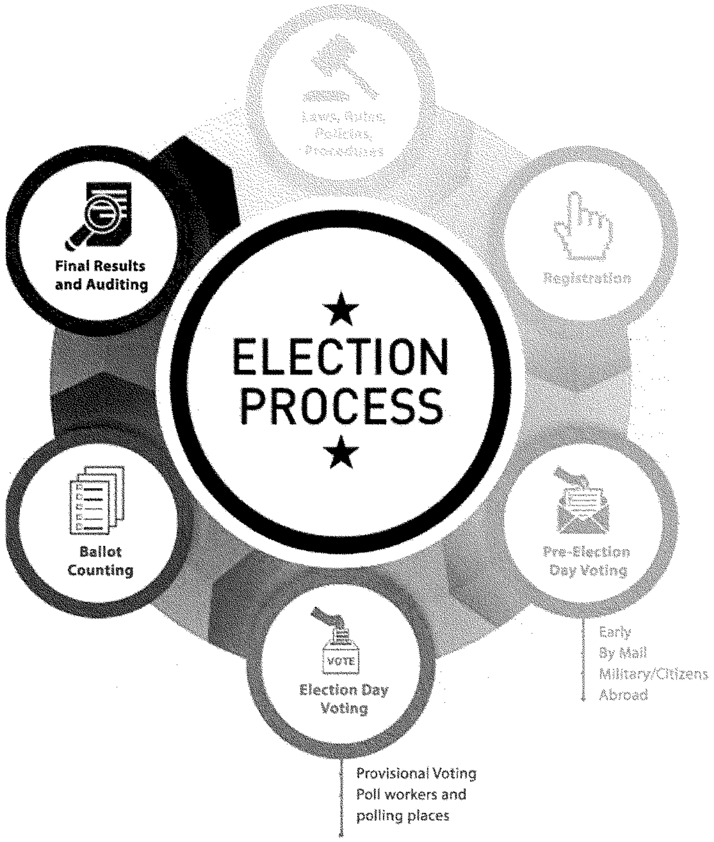


FIGURE 3-1 The U.S. election process.
SOURCE: Adapted from U.S. Election Assistance Commission, *2016 Election Administration and Voting Survey* (EAVS), June 29, 2016, p. 4. The original image, which is available at: https://www.eac.gov/assets/1/6/2016_EAVS_Comprehensive_Report.pdf, is the work of the U.S. Election Assistance Commission, taken or made during the course of an employee's official duties. As a work of the U.S. federal government, the image is in the public domain.
NOTE: This figure is provided as a general illustration of the election process. It does not include all components of the process, e.g., poll site selection.

political parties hold so-called primary elections. In primary election scenarios, candidates compete to stand as their party's single nominee in the general election.[3] In jurisdictions that hold non-partisan elections, a first round known as a preliminary election is held to reduce the number of candidates prior to the general election.

The large number of elections and the numerous contests on many ballots create an administrative challenge to election administrators. This challenge is a principal driver for automation in American election administration.

The details of election administration vary considerably across states and local governments. Variation exists with respect to levels of funding,[4] human resources, how ballots are cast, and how votes are captured and tabulated. Furthermore, federal and state laws govern how military and overseas citizens may cast their votes in absentia.[5] The result is a diverse and complex system of elections and wide variation in the training and capability of election administrators and staff who administer elections.

On Election Day, problems can arise when the lines to vote are too long, when voting rolls are inaccurate, when voting machines break down, when ballots are poorly designed, when physical accessibility is limited, when precincts run out of ballots, when poll workers are poorly trained, or when election systems are compromised.[6] Equipment failure, inadequate training, or poor ballot design can lead to long wait times. Inadequate access for voters with limited English proficiency or for voters with disabilities may be the result of insufficient resources applied to the needs of those communities. Inaccurate voter registration lists may stem from the absence of comprehensive and current voter registration databases. Election systems may be vulnerable to intrusions that target voter rolls or voting systems.

To ensure that the results of an election are representative of the will of the people, every valid vote must be accurately counted. To achieve this, eligible citizens must be able to obtain their ballots, cast their votes for their candidates of choice, and have those votes recorded and tabulated accurately. At the same time, repeat voting and voting by ineligible individuals must be deterred and prevented.

[3] In a few states, for some offices, political parties still hold conventions to nominate party representatives in the general election.

[4] It is extremely challenging to calculate the cost of election administration in the United States (see Appendix D).

[5] The primary federal laws affecting voting by military and overseas civilians are the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), Pub.L. 99-410, and the Military and Overseas Voter Empowerment Act (MOVE), Pub.L. 111-84. Both of these laws are overseen by the Federal Voting Assistance Program (FVAP), which is a part of the U.S. Department of Defense. See https://www.fvap.gov.

[6] In addition to reliability issues and issues relating to the management of the flow of voters, Election Day problems may include issues related to election integrity and voter privacy.

In modern elections, the voting process is largely dependent on technology-based systems known as election systems. These systems collect, process, and store data related to all aspects of election administration.[7] Election systems include public election websites (e.g., state "my voter" pages),[8] voter registration (VR) systems, voting systems (the means through which voters cast their ballots), vote tabulation systems, election night reporting systems, and auditing systems (see Figure 3-2).[9]

In the United States, votes are cast: (1) in person; (2) via mail;[10] or (3) digitally from a remote location.[11] Regardless of how a vote is cast, each voter is assigned to a voting district, typically called a precinct, which is a bounded geographic area wherein all individuals generally vote for the same set of candidates and issues. In all cases, an individual must meet eligibility requirements and, in most states, must be registered to vote before he or she may be able to cast a lawful ballot.[12]

VOTER REGISTRATION, VOTER REGISTRATION DATABASES, AND POLLBOOKS

Voter registration plays a central role in elections in 49 states and the District of Columbia,[13] as in these locations, a voter must be registered for his or her vote to count. [14] As a general rule, voters register to vote in a spe-

[7] King, Merle, Kennesaw State University, PowerPoint presentation to the committee (Slide 5), June 12, 2017, New York, NY. The presentation is available at: http://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_180929.pdf.

[8] Georgia's My Voter Page, for instance, provides information on the state administration of elections and elections results and allows individuals to check their voter registration status, mail-in application and ballot status, and provisional ballot status; to locate poll and early voting locations; and view information about elected officials and sample ballots for upcoming elections. See https://www.mvp.sos.ga.gov/MVP/mvp.do.

[9] King, Slide 5.

[10] Vote-by-mail ballots are often returned by voters at central drop-off points unconnected to the United States Postal Service. See discussion below addressing vote-by-mail directly.

[11] Digital return of ballots for counting is rare, and is primarily done in the case of some overseas ballots in a limited number of jurisdictions.

[12] North Dakota does not require voter registration. In some jurisdictions, registration may be automatic or available at the time of voting.

[13] Throughout this report, reference is made to statistics that include American states and the District of Columbia but not U.S. territories or commonwealths. This is due to the fact that some of the most authoritative data sources pertaining to election administration are inconsistent in the inclusion of data from territories/commonwealths.

The U.S. Election Assistance Commission's *Election Administration and Voting Survey* cited in this report, includes data provided by four territories—American Samoa, Guam, Puerto Rico, and the Virgin Islands—but does not include data from the Northern Mariana Islands.

[14] As mentioned in a previous footnote, North Dakota does not require voter registration. Rather, in North Dakota, voters need only provide photo identification and proof of age and residency at the time they vote.

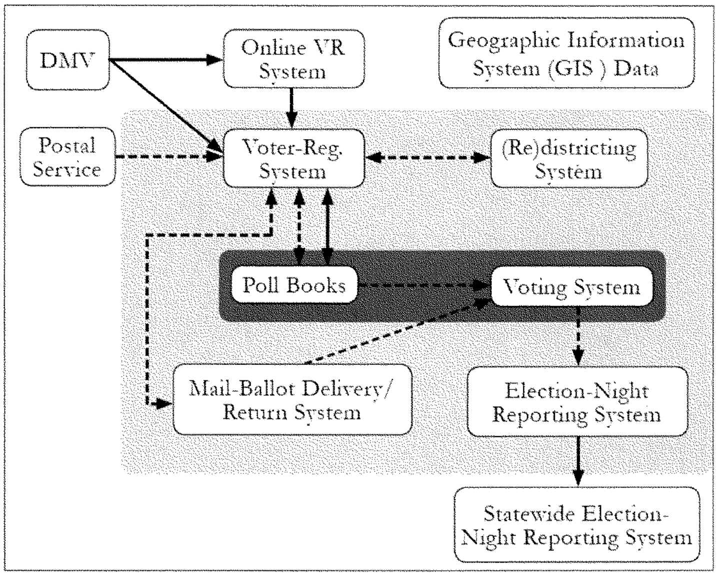

DMV
Online VR System
Geographic Information System (GIS) Data
Postal Service
Voter-Reg. System
(Re)districting System
Poll Books
Voting System
Mail-Ballot Delivery/ Return System
Election-Night Reporting System
Statewide Election-Night Reporting System

FIGURE 3-2 The interaction of election systems.
SOURCE: Stewart, Charles III, "The 2016 U.S. Election: Fears and Facts About Electoral Integrity," *Journal of Democracy,* April 2017, Vol. 28, No. 2, p. 56, Figure 2. © 2017 National Endowment for Democracy and Johns Hopkins University Press. Reprinted with permission of Johns Hopkins University Press.
NOTES: This schematic of voting information-system architecture is based on the work of Merle King. As a schematic, it does not include all conceivable election systems, e.g., systems used to pre-program ballot designs. For King's original figure, see http://www.nist.gov/sites/default/files/documents/itl/vote/tgdc-feb-2016-day2-merle-king.pdf (p. 14).
Arrows depict the direction of information flow between component systems. Solid lines indicate flows that typically rely on the Internet or other networks that are connected to the Internet; dashed lines indicate information flows that typically are "air-gapped" from outside networks. The dark box indicates systems that are typically deployed in individual polling places; the light-gray box indicates systems that are typically centralized in a local jurisdiction's election office.

cific geographic jurisdiction that is determined from the residential address that they provide for the purpose of voting. The voting address of record determines the voting district wherein a voter may cast a ballot. States set deadlines for when a voter must register to participate in an election.

Individuals may register to vote in many ways. They may register in person at election offices or at temporary sites set up in public places. They may register at departments of motor vehicles, departments of human services, and public assistance agencies.[15] All states offer the option to register to vote by mail. In 37 states and the District of Columbia, individuals can register to vote via the Internet so long as the registrant's information can be matched to information that was provided when a driver's license or other state-issued identification was issued.[16] Overseas voters and members of the U.S. armed forces and their dependents may obtain registration forms via electronic transmission.[17] Fifteen states currently allow same-day voter registration, and another, Hawaii, has enacted same-day registration provisions that take effect in 2018.[18] Nine states and the District of Columbia have introduced automatic voter registration (AVR).[19]

The 2002 Help America Vote Act (HAVA) established a requirement that all states implement a "single, uniform, official, centralized, interactive computerized statewide voter registration list." The list is to be administered by the state and contain the "name and registration information of every legally registered voter in the state."[20] To function as intended, each state voter registration database (VRD) must (1) add new registrants to the VRD; and (2) update information about voters (e.g., name and address changes).[21] These tasks require both good data and good matching procedures.

[15] The "Election Administration and Voting Survey: 2016 Comprehensive Report" (EAVS) states that, while state motor vehicle offices are the most common place where individual register to vote with 32.7 percent of all registrations, online registration has increased dramatically over the past 4 years (see p. i).

[16] See http://www.ncsl.org/research/elections-and-campaigns/electronic-or-online-voter-registration.aspx. Oklahoma has passed legislation to create online voter registration, but has yet to implement online voter registration.

[17] A subtitle of the National Defense Authorization Act for Fiscal Year 2010 (Pub.L. 111-84), the Military and Overseas Voter Empowerment Act ("MOVE" Act), required each state to designate not less than 1 means of electronic communication…for use by absent uniformed services voters and overseas voters who wish to register to vote or vote in any jurisdiction in the State to request voter registration applications." See Sec. 577.

[18] See http://www.ncsl.org/research/elections-and-campaigns/same-day-registration.aspx.

[19] "Automatic voter registration is an 'opt out' policy by which an eligible voter is placed on the voter rolls at the time they interact with a motor vehicle agency (or, in a few states, with other government agencies) unless they actively decline to be registered." See http://www.ncsl.org/research/elections-and-campaigns/automatic-voter-registration.aspx.

[20] HAVA § 303, 52 U.S.C. § 21083.

[21] Because voter registration lists are maintained by individual states, when a voter moves from one state to another, registration information does not follow the voter. As a consequence, the voter must register in his or her new state. Although voter registration forms ask new registrants whether they are registered in another state, the law does not require a voter to answer this question. As a result, it is common for individuals to appear on registration rolls in more than one state, even though they are only eligible to vote in one.

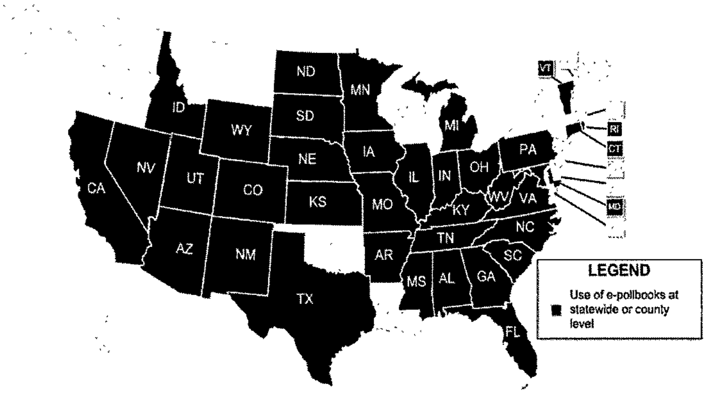


FIGURE 3-3 Electronic pollbook usage in the United States.
SOURCE: Adapted from Matthew Masterson, U.S. Election Assistance Commission, presentation to the committee, April 5, 2017, Washington, DC. The original image, which is available at: http://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_178367.pdf, is the work of the U.S. Election Assistance Commission, taken or made during the course of an employee's official duties. As a work of the U.S. federal government, the image is in the public domain.

The VRD is used to prepare pollbooks. Pollbooks are used at polling places to verify an individual's eligibility to vote at the location where they have appeared. Traditionally, pollbooks were lists of registered voters that were printed and distributed to polling places in advance of an election, but increasingly, jurisdictions are using electronic pollbooks (EPBs or e-pollbooks). E-pollbooks are typically housed on laptops or tablets. Some contain local, static lists in electronic form, while others allow access to information in voter registration databases via a real-time Internet connection. According to the U.S. Election Assistance Commission, 36 states now use e-pollbooks (see Figure 3-3) in at least some of their jurisdictions.

BALLOTS

Across the country, jurisdictions use a variety of ballots (paper, card, or electronic) to present candidates and issues to voters. Ballots are often designed under multiple "constraints, including state laws on structure and ballot access rules, minority language requirements for jurisdictions covered by the VRA, the type of voting equipment used, and the various combinations of offices and issues for which people are eligible to vote."[22] Such constraints complicate the ballot design process.

A provisional ballot may be used to record the individual's vote if a voter's eligibility to vote cannot be established or if an election official asserts that the individual is not eligible to vote. Provisional ballots are required under HAVA, but states establish the criteria under which an individual may obtain a provisional ballot (see Appendix E).[23] Votes cast with provisional ballots are counted only after a voter's eligibility to vote has been established.

POLL WORKERS

On Election Day, paid temporary workers assist in polling place operations. These poll workers may verify the identity of a voter; assist voters in signing the register, affidavits, or other documents required to cast a ballot; provide a ballot to a voter; set up a voting machine; or carry-out other functions as dictated by state law.[24]

Many jurisdictions have difficulty recruiting and training poll workers because this "seasonal" work involves "long hours, low pay, workday conflicts that limit the recruiting pool, and increasing technological demands for special skills."[25] In 2016, "46.9 percent of responding jurisdictions reported having a somewhat difficult or very difficult time recruiting poll workers, compared with 22.7 percent that reported having a somewhat easy or very easy time. States and territories reported deploying an aver-

[22] Montjoy, Robert S., "The Public Administration of Elections," *Public Administration Review*, September-October 2008, pp. 792-793.

[23] See http://www.ncsl.org/research/elections-and-campaigns/provisional-ballots.aspx. Idaho, Minnesota, New Hampshire, North Dakota, Wisconsin, and Wyoming were exempt from the HAVA provisional ballot requirement as these are states that offered same day registration in 2002, the year HAVA was enacted. Nonetheless, some states that are not required to use provisional ballots have provisions for their use, and several states used provisional ballots before HAVA was enacted.

States where all ballots are returned by mail provide for the casting of provisional ballots. In Oregon, if a voter has a question about his or her eligibility to vote, he or she may request a provisional ballot from any Oregon County Elections Office (see http://sos.oregon.gov/elections/Documents/SEL113.pdf). In Washington, provisional ballots may be cast at any voter service center (see https://wei.sos.wa.gov/county/spokane/en/pages/FrequentlyAskedQuestions.aspx). Likewise, in Colorado, provisional ballots may be cast at voter service and polling centers (see https://www.sos.state.co.us/pubs/elections/FAQs/ElectionDay.html).

[24] "2016 Election Administration and Voting Survey" (EAVS), p. 13.

[25] U.S. Government Accountability Office, "Elections: Perspectives on Activities and Challenges Across the Nation" (Washington, DC: Government Printing Office, 2001), available at: https://www.gao.gov/new.items/d023.pdf.

In addition, poll workers must ensure compliance with numerous polling place mandates.

age of 7.8 poll workers per polling place for Election Day 2016."[26] Data provided on approximately 53 percent of poll workers who served in the 2016 federal election indicates that the poll worker population is skewed toward older individuals. Most poll workers are over age 40, 32 percent were between the ages of 61 and 70, and 24 percent were 71 years of age or older.[27]

While the qualifications required of poll workers vary by state, poll workers must often be registered to vote in the precinct or county in which they will serve. They must often also meet specific bilingual language requirements.

CASTING A VOTE

Voting Systems and the Voting Technology Marketplace

In the United States, voters cast votes using a variety of voting systems (see Figure 3-4). As discussed in Box 3-1, voting systems can be distinguished by the means of casting and tabulating votes. Voters have long cast their votes on paper (see Box 3-2), and paper remains the most commonly used medium in vote casting. The great majority of paper ballots are marked by the voter, and voter responses are tabulated using computerized optical scanners in a manner that is similar to systems used to record answers to standardized tests.[28] Alternatively, ballot-marking devices (BMDs) may be used in conjunction with optical scanners. In this scenario, a voter uses a touchscreen or keypad to select his or her choices on a digital display. When the voter has completed the selection process, a paper copy of the completed ballot is printed. This ballot can be scanned optically or digitally, but can also be read by humans. BMDs do not tabulate votes or record them in a computer's memory. Instead, the paper ballots are scanned and tabulated using a separate device.

Optical scan systems were the most commonly used voting system in U.S. counties in the 2016 election (see Table 3-1). In about one-third of U.S. counties, voters cast their ballots using BMDs or Direct Recording Electronic (DRE) systems where the voter casts his or her ballot using an electronic system (often similar to an ATM) (see Table 3-1). With DREs, ballots are then counted internally by the system's computer. In a small percentage of counties, voters either cast paper ballots that were manu-

[26] "2016 Election Administration and Voting Survey" (EAVS), p. 13.

[27] Ibid, p. 14.

[28] There are important differences. With standardized tests, for example, there are examination booklets with questions and separate sheets where students mark their selected answer by filling in ovals that correspond with their intended answer. With ballots, responses are marked by filling in ovals adjacent to the names of candidates or other choices.

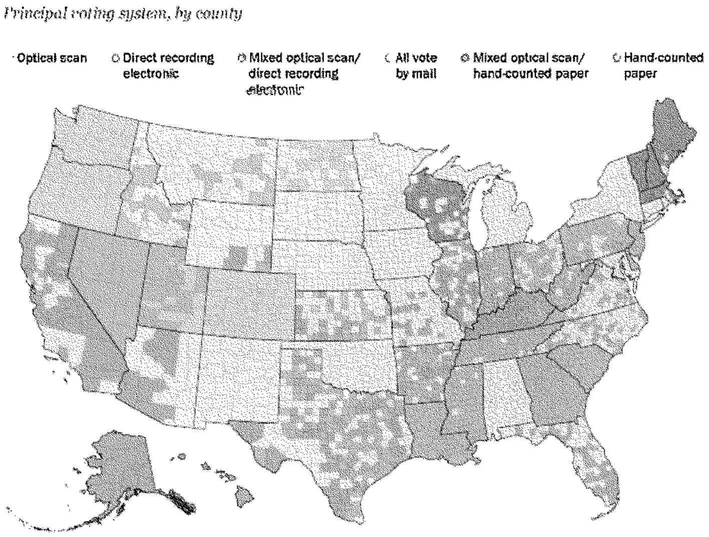

Principal voting system, by county
Optical scan
Direct recording electronic
Mixed optical scan/ direct recording electronic
All vote by mail
Mixed optical scan/ hand-counted paper
Hand-counted paper

FIGURE 3-4 Voting systems across the United States.
SOURCE: Desilver, Drew, "On Election Day, Most Voters Use Electronic or Optical-Scan Ballots," Pew Research Center, November 8, 2016. Pew Research Center created the figure using data from the Verified Voting Foundation.

BOX 3-1
Overview of Vote Casting and Tabulation Methods

Systems in Use in Federal Elections

Hand-Marked "Optical" Scan Paper Ballot Systems. Voters mark paper ballots that are subsequently recorded electronically by scanning devices. On most scanned ballots, voters indicate their selections by filling in an oval or completing an arrow. Ballots may either be scanned on precinct-based optical scan systems in a polling place (precinct count) or collected in a ballot box to be scanned at a central location (central count). The original generation of optical ballot scanners used one row of optical sensors, one sensor per ballot column, to detect the voters' marks. Newer ballot scanners, sometimes referred to as "digital scanners," store an electronic image of each ballot [a "cast vote record" (CVR)], which can be used later if auditing of the election process is required.[a] The original generation

BOX 3-1 Continued

of ballot scanners used infrared sensors to detect ballot marks, giving rise to the generic term "optical scanner." Optical scanners are still used even though newer image-processing technologies are available.

Direct Recording Electronic (DRE) Systems. Voters use an electronic interface to record their votes directly into a computer's memory (e.g., onto a memory cartridge or memory card). That computer counts the vote. A keyboard is typically provided to allow entry of write-in votes, though older models have a paper roll behind a small opening where voters record write-in votes using a pen.

The first generation of DREs used a push-button interface, while later systems use a touchscreen interface or a dial interface.[b]

Some DREs are equipped with a voter-verifiable paper audit trail (VVPAT) feature that prints the voter's selections on paper and allows voters to confirm their selections by inspecting this paper before their votes are cast. The paper record is preserved and, depending on state election codes, may serve as the ballot of record in the event of an audit or recount.

Machine-Marked Paper Ballot Systems. A growing number of jurisdictions are using electronic "ballot-marking devices" (BMDs), which use electronic devices to mark paper ballots according to voters' instructions. The paper ballots are usually counted by optical scanners.

Hand Counted Paper Ballots. A small number of jurisdictions continue to manually count paper ballots cast in polling places.

Systems No Longer In Use In Federal Elections

Punch Card Voting Systems. Those systems employed a card (or cards) and a small clipboard-sized device for recording votes. Voters marked their choice by punching holes in the cards with a punch device. After voting, the voter either placed the ballot in a ballot box for later tabulation or the ballot was fed into a vote-tabulating device at the precinct. No jurisdictions used punch card voting systems in federal elections in 2016.

Mechanical Lever Voting Machines. First introduced in the 1890s, mechanical lever machines were used in many states during the 20th century. Voters would make choices by flipping levers and their selections were tabulated on machine counters similar to automobile odometers. As recently as 1996, mechanical lever machines were used by 20.7 percent of registered voters in the United States. Since 2010, no mechanical lever voting machines have been used in federal elections.

[a] Some scanners also store a digital photograph of the ballot.

[b] See Jones, Douglas W. and Barbara Simons, *Broken Ballots: Will Your Vote Count?* (Stanford: Center for Language and Information, 2012), pp. 91-101.

BOX 3-2
The Role of Paper in Elections

Until the widespread adoption of mechanical lever machines in the mid-20th century, hand-marked paper had been the most common medium upon which a voter cast a ballot. The cast paper ballot provided a physical record that could be examined in instances where a recount or other reconciliatory action was required. With the advent of mechanical lever machines, no record of a voter's choices was permanently stored, either on paper or mechanically—the only effect of casting a vote was to increment mechanical counters that accumulated the choices made by voters on a particular machine. Mechanical lever machines were popular where they were used. However, these machines were prone to breakdowns that could go undetected until balloting had ended.

Before the passage of the Help America Vote Act (HAVA), it was common for jurisdictions with lever machines to adopt electronic systems when they considered upgrading their voting systems. HAVA provided an impetus for jurisdictions that had previously used lever machines to adopt Direct Recording Electronic systems (DREs), either to provide accessible options for those with disabilities, or to replace paper-based systems altogether. The rapid growth in the prominence of DREs brought greater voice to concerns about their use, particularly their vulnerability to software malfunctions and external security risks. And as with the lever machines that preceded them, without a paper record, it is not possible to conduct a convincing audit of the results of an election.

Many electronic voting systems utilize paper as part of their operation. As discussed in Box 3-1, voters may mark paper ballots that are subsequently recorded electronically by scanning devices. Alternatively, ballot-marking devices may be used to mark paper ballots according to voters' instructions. In the case of DREs, there is no physical (i.e., paper) ballot. Instead, the ballot exists only in electronic form.

Problems arise when a voter does not actually verify his or her ballot, especially when the ballot is being tabulated by a computer that has a software flaw or is infected with malware (see Chapter 5). A ballot that is "voter marked" is by definition voter verified. Voters can verify that the selections on hand-marked ballots or on paper ballots produced by BMDs reflect their intended choices before their votes are tabulated. With DREs, voters may similarly verify their selections using a voter-verifiable paper audit trail (VVPAT) (see Box 3-1)—provided that the DRE is equipped with this feature. The information on a VVPAT may accurately present a voter's selections, but VVPATs exist independently of the record maintained in the DRE's computer memory. In most cases it is the electronic record, and not the VVPAT, that is used for vote tabulation.[a]

Paper Ballots Defined

Because records of ballots may take many forms, it is important to clearly define what is meant by "paper ballot." For the purposes of this report, references to paper ballots refer to original records that are produced by hand or a ballot-marking device, which are human-readable in a manner that is easily accessible for inspection and review by the voter without any computer intermediary (i.e., voter-verifiable), countable by machine (such as a scanner) or by hand, and which may be recounted or audited by manual examination of the human-readable portion of the ballot.

A paper ballot–based voting system makes the paper ballot the official "ballot of record" of the voter's expressed intentions. Other representations (e.g., an electronic representation produced by a scanner) are derivative and are not voter-verifiable. The human-readable portion of the cast paper ballot provides the basis for audits and recounts.

The Challenges of Paper Ballots

The use of hand-marked paper ballots can introduce voting errors. Voters may inadvertently make stray marks that can be misread by optical scanners. Voters using hand-marked paper ballots may accidentally skip a race or vote for multiple candidates in a race and thereby invalidate their vote for that particular race.[b] Counting paper ballots can be tedious, leading to vote-count errors.[c]

Paper ballots are not immune to fraud. Fraud may occur through ballot theft, destruction, or substitution, by ballot-box stuffing, or by the addition of marks to ballots after a voter finishes voting.[d]

Paper ballots can present logistical challenges when used in vote centers and in early voting, especially in densely populated, metropolitan areas. In vote centers and in early voting, every jurisdiction-specific ballot "style" that might conceivably be requested by a voter in a jurisdiction must be available at every voting site. In smaller jurisdictions, this functional requirement can be satisfied by having a physical inventory of every ballot style that might be requested at a site, through what is known as a "pick-and-pull" system. In larger jurisdictions that might have hundreds of ballot styles, maintaining a complete, secure inventory of ballot styles in every voting location may be logistically impossible or cost-prohibitive. One solution to this problem is a "ballot-on-demand" system, where appropriate ballots are printed on the spot for every voter. However, certain ballot-on-demand systems are costly and can put significant strain on the electrical systems of buildings hosting these systems.[e]

Electronic voting systems introduce challenges in and of themselves. Such systems are, for example, more costly than systems that use paper exclusively. Technical support for such systems is often necessary and adds to their cost over time. Such systems may also be more prone to breakdowns, are subject to technological obsolescence, and as is discussed in Chapter 5, vulnerable to cyberattacks and other threats. Furthermore, electronic systems must be stored in secure locations when not in use.

[a] As noted in Box 3-1, in some states, when a VVPAT is produced by a DRE, the VVPAT may be used as the ballot of record for election contests and recounts.

Research suggests that DRE VVPATs tend not to be voter verified. This suggests that VVPATs may be of little value as a check on the accuracy of DREs. See, e.g., Everett, S. P., "The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection," doctoral dissertation, Rice University, Houston, Texas and Campbell, Bryan A. and Michael D. Byrne, "Now Do Voters Notice Review Screen Anomalies? A Look at Voting System Usability," *Proceedings of EVT/WOTE*, 2009.

continued

BOX 3-2 Continued

Research on the rate of voter verification of BMD ballots relative to the rate of verification of VVPATs or voter-marked paper ballots has been limited.

[b] Voters may also accidentally skip races when using DREs (see Chapter 4).

[c] For a discussion of the inherent weaknesses in human vote counting, see Goggin, Stephen N., Michael D. Byrne, and Juan E. Gilbert, "Post-election Auditing: Effects of Procedure and Ballot Type on Manual Counting Accuracy, Efficiency, and Auditor Satisfaction and Confidence," ***Election Law Journal: Rules, Politics, and Policy,*** 2012, Vol. 11, No. 1, pp. 36-51. A recount or audit can make use of limited software (e.g., spreadsheets) to assist in the counting.

Dr. Gilbert is a member of the committee that authored the current report.

[d] Such fraud provided motivation for the adoption of mechanical lever voting machines in the late 19th century.

[e] Power usage is determined by the type of printer required to produce the desired ballot. In instances where a printer must create an entire blank ballot certified to meet particular specifications using paper of a specific quality, be digitally readable, and be assigned a unique serial number, the necessary printer may draw significantly more power than is typical for printers used to print only voter selections on archival thermal paper.

TABLE 3-1 Types of Voting Systems Used in the United States in 2016

Voting System	Percent of U.S. Counties Using System
Hand Counted Paper Ballot	1.54%
Optical Scan	62.78%
Electronic (DRE or BMD)	32.85%
Mixed	2.69%

SOURCE: Brace, Kimball, President, Election Data Services, Inc., "The Election Process from a Data Perspective," presentation to the Presidential Advisory Commission on Election Integrity, September 12, 2017, Manchester, NH, available at: https://www.electiondataservices.com/wp-content/uploads/2017/09/BracePresentation2PenseCommAmended.pdf.

ally counted or voted with a mixture of systems (see Table 3-1). In many instances, marked ballots are submitted by mail and tabulated at a central location.

HAVA requires that each polling place used in a federal election

> be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) [29] as for other voters . . . through the use of at least one

[29] Participation also includes the ability to cause one's own ballot selections to be recorded, verifying that one's ballot selections are correctly recorded, and the casting of one's self-verified ballot.

> direct recording electronic voting system or other voting system equipped for individuals with disabilities at each polling place.[30]

Practically speaking, this means that even in local jurisdictions where ballots are typically cast by paper, DREs or other accessible voting systems are available in all polling places to comply with HAVA's accessibility requirements.

Further, HAVA requires that voting systems provide alternative language accessibility.[31] HAVA does not, however, provide a private right of action for voters with disabilities to pursue enforcement of either the disability or alternative language access provisions.[32] The 1990 Americans with Disabilities Act (ADA) may, however, provide a private right of action.[33]

Currently, there are only a few manufacturers of election systems. In the United States, three firms comprise 92 percent of the voting system market by voter reach.[34] The largest firm has about 460 employees.[35] This concentration represents a potential security risk, as a successful malicious infiltration of a single company could affect the operations of a significant portion of the election systems in use.

Certification of voting systems is an authority that rests with the states, although an important role in certification is played by the U.S. Election Assistance Commission (EAC) and the National Institute for Standards and Technology (NIST). Working collaboratively, the EAC and NIST maintain the Voluntary Voting System Guidelines (VVSG), which are a set of specifications against which voting systems are tested and which states may voluntarily adopt, in part or as a whole.[36] Several states require either testing to meet federal standards or testing by a federally accredited laboratory, and many states require full federal certification. In addition, many states have certification standards that meet or exceed federal standards (see Table 3-2).

[30] HAVA § 301(a)(3), 52 U.S.C. § 21081(a)(3).

[31] See HAVA § 301(a)(4), 52 U.S.C. § 21081(a)(4).

[32] See Golden, Diane Cordry, Association of Assistive Technology Act Programs, PowerPoint presentation to the committee (Slide 3), June 13, 2017, New York, NY. The presentation is available at: http://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_180932.pdf.

A private right of action is the right to bring a lawsuit.

[33] 42 U.S.C. §§ 12101 *et seq.*

[34] See University of Pennsylvania Wharton School, "The Business of Voting: Market Structure and Innovation in the Election Technology Industry," 2016, available at: https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

The three firms are Elections Systems & Software, Dominion Voting Systems, and Hart InterCivic.

[35] Ibid. That firm is Elections Systems and Software.

[36] The current version of the Voluntary Voting System Guidelines, VVSG1.1, was adopted by U.S. Election Assistance Commission commissioners on March 31, 2015. It is anticipated that the next iteration of the guidelines, VVSG 2.0, will be adopted in 2018. See https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/.

TABLE 3-2 Voting Systems Certification Standards by State

States Requiring Testing to Federal Standards	States Requiring Testing by a Federally Accredited Laboratory	States Requiring Full Federal Certification (in Statute or Rule)
Connecticut, DC, Hawaii, Indiana, Kentucky, Nevada, New York, Tennessee, Texas, and Virginia	Alabama, Arkansas, Arizona, Colorado, Illinois, Iowa, Louisiana, Massachusetts, Maryland, Michigan, Minnesota, Missouri, New Mexico, Oregon, Pennsylvania, Rhode Island, Utah, and Wisconsin	Delaware, Georgia, Idaho, North Carolina, North Dakota, Ohio, South Carolina, South Dakota, Washington, West Virginia, and Wyoming

The following four states refer to federal agencies or standards, but do not fall into the categories above: Alaska,[a] California,[b] Kansas, and Mississippi.[c, d]

The following eight states have no federal testing or certification requirements. Statutes and/or regulations make no mention of any federal agency, certification program, laboratory, or standard; instead these states have state-specific processes to test and approve voting systems: Florida, Maine, Montana, Nebraska, New Hampshire, New Jersey, Oklahoma, and Vermont.

[a] In Alaska, the state elections director may consider whether the Federal Election Commission (FEC) has certified a voting machine when considering whether the system shall be approved for use in the state (though FEC certification is not a requirement).

[b] In California, the Secretary of State adopts testing standards that meet or exceed the federal voluntary standards set by the U.S. Election Assistance Commission.

[c] Mississippi requires that Direct Recording Electronic (DRE) systems shall comply with the error rate standards established by the FEC (though other standards are not mentioned).

[d] Even states that do not require federal certification typically still rely on the federal program to some extent and use voting systems created by vendors that have been federally certified.

SOURCE: Adapted from National Conference of State Legislatures, "Voting System Standards, Testing and Certification," available at: http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx.

The software used to operate voting systems is generally proprietary; its purchase is bundled with the purchase of hardware and maintenance services.[37] The software installed on commercial election systems typically runs on a commercial off-the-shelf (COTS) operating system that is usually proprietary. There is a movement by some election administrators to

[37] Proprietary software is owned by a company or individual. The owner(s) of proprietary software typically place restrictions on how the software may be used. Users of proprietary software and other individuals outside of the company generally do not have access to the software's source code. As a result, they cannot modify the source code or view it to identify flaws or vulnerabilities.

Some states require the code to be escrowed and accessible for inspection in specified circumstances.

BOX 3-3
U.S. Government Accountability Office Survey on Voting Equipment Use and Replacement

In a recent survey, the United States Government Accountability Office (GAO) "identified four key factors that jurisdictions and states consider when deciding whether to replace voting equipment[a]—(1) need for equipment to meet federal, state, and local voting system standards and requirements; (2) cost to acquire new equipment and availability of funding; (3) ability to maintain equipment and receive timely vendor support; and (4) overall performance and features of equipment."[b]

The survey also found that local election jurisdictions using "optical scan and direct recording electronic (DRE) . . . equipment during the 2016 general election . . . were generally satisfied with voting equipment performance." "Survey results indicated that accurate vote counting and efficiency of operation were top benefits experienced by jurisdictions for both types of equipment, and storage and transportation costs were a top challenge."[c]

In addition, stakeholders including state officials and voting equipment vendors "generally indicated that [. . . voluntary federal voting system] guidelines and their associated testing processes provide helpful guidance for equipment developers, cost savings for states that do not have to duplicate federal testing, and assurance that certified equipment meets certain requirements. However, some of these stakeholders stated that aspects of the guidelines could discourage the development of innovative equipment and limit the choices of voting equipment on the market." [d,e]

[a] The GAO report defines voting equipment as "the method or machine used to create ballots, cast and count votes, report election results, and maintain and produce audit trail information. It does not include other voting-related systems, such as those used for voter registration." See U.S. Government Accountability Office, "Observations on Voting Equipment Use and Replacement," April 11, 2018 (Washington, DC), p. 1, available at: https://www.gao.gov/products/GAO-18-294.

[b] Ibid, "Highlights of GAO-18-294."

[c] Ibid.

[d] Ibid.

[e] Ibid. For the survey, "GAO surveyed officials from a nationwide generalizable sample of 800 local jurisdictions (68 percent weighted response rate) and all 50 states and the District of Columbia (46 responded) to obtain information on voting equipment use and replacement. GAO also interviewed officials from (1) five jurisdictions, selected based on population size and type of voting equipment used, among other things, to illustrate equipment replacement approaches; and (2) seven voting system vendors, selected based on prevalence of jurisdictions' use of equipment, type of equipment manufactured, and systems certified, to obtain views on federal voting system guidelines."

develop or adopt open-source or publicly owned software that is available in source code form with a license, allowing the source code to be studied, modified, and distributed without limitation.[38] Open-source software is typically installed on commercial off-the-shelf equipment.

Election administrators take many factors into account when purchasing voting systems (see Box 3-3). Jurisdictions typically enter into software licensing and maintenance agreements with the vendors of commercial equipment. In exchange, the vendor maintains and provides hardware support for the election system and provides support for and upgrades to its proprietary software. In many jurisdictions, commercial vendors also provide the digital ballot definitions that enable their equipment to present, print, scan, and tabulate the jurisdiction's election-specific ballots for those casting votes.

Absentee Voting and Voting by Mail

Historically, voters were required to cast their ballots in person at their assigned polling places on Election Day. Absentee voting was originally developed to allow soldiers deployed away from home to vote. Eventually, the use of absentee ballots was extended to civilian voters, utilizing the mails to transmit and return ballots.[39]

Originally, voters had to provide an acceptable excuse to cast an absentee ballot, e.g., illness or travel. Today, however, most states have broadened voting mechanisms for the convenience of voters. Most states allow early in-person voting or voting by mail without requiring an excuse (see Figure 3-5).[40]

Three states, Washington, Oregon, and Colorado, have adopted mail-only voting. In these states, ballots are mailed to all registered voters. Voters may return completed ballots either by mail or in person. In 2016, most voters in these three states returned their ballots in person, rather than via

[38] Travis County in Texas, San Francisco, and Los Angeles County in California are three jurisdictions that are exploring the use of open-source operating systems. The state of New Hampshire recently adopted an open-source system called One4All based upon open-source software called Prime III developed at the University of Florida. Dr. Juan E. Gilbert, who serves as a member of the committee that authored the current report, was a developer of Prime III.

Software developers may also opt to make underlying source code available for others to review but not to modify without explicit permission. This scenario is sometimes referred to as disclosed source.

[39] Inbody, Donald S., *The Soldier Vote: War, Politics, and the Ballot in America* (New York: Palgrave Macmillan, 2016).

[40] Some states call all voting by mail early voting, whereas others refer to in-person early voting as a form of absentee voting. The use of different terms for what are essentially the same processes lends confusion to discussions of absentee or early voting.

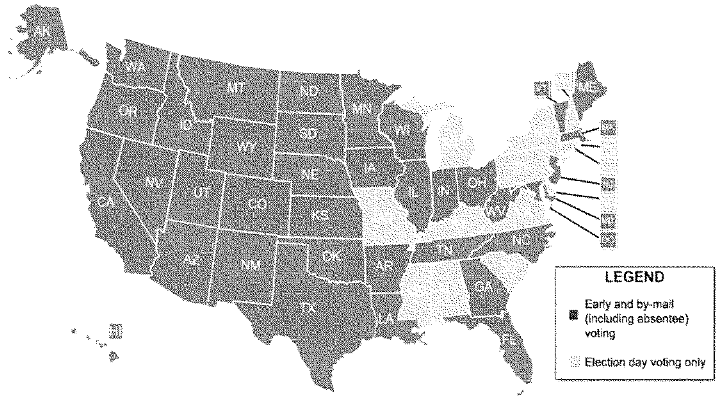


FIGURE 3-5 Early and by-mail (including absentee) voting in the United States.
SOURCE: Adapted from Masterson, Matthew, U.S. Election Assistance Commission, presentation to the committee, April 5, 2017, Washington, DC. The original image, which is available at: http://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_178367.pdf, is the work of the U.S. Election Assistance Commission, taken or made during the course of an employee's official duties. As a work of the U.S. federal government, the image is in the public domain.
NOTE: For states designated as allowing "Election Day voting only," ballots received early may be cast if specific criteria are met.

the mail.[41] Thus, it is actually a misnomer to refer to these as "vote-by-mail" states. It is more accurate to refer to them as "ballot-delivery-by-mail" states.

Two other states, California and Utah, are moving toward mail-only elections. Currently, most voting in these states is conducted by mail.[42] In

[41] Stewart, Charles III, "2016 Survey of the Performance of American Elections: Final Report," 2017, p. 26. Dr. Stewart is a member of the committee that authored the current report.

[42] Masterson, Matthew, U.S. Election Assistance Commission, presentation to the committee, April 5, 2017, Washington, DC. See also "2016 Election Administration and Voting Survey" (EAVS), p. 9.

There are accommodations for in-person voting in the three states that conduct their elections by mail. In Washington, every county has a vote center for in-person voting (see https://www.sos.wa.gov/elections/faq_vote_by_mail.aspx). In Oregon, each County Elections Office provides privacy booths for voters who want to vote in person or voters who need assistance (see https://multco.us/file/31968/download). In Colorado, voters have the option to vote in person at a county Voter Service and Polling Center (VSPC) (see https://www.sos.state.co.us/pubs/elections/FAQs/ElectionDay.html).

2016, 52 percent of California's ballots and 68 percent of Utah's ballots were cast by mail.[43]

In addition, the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) allows "U.S. citizens who are active members of the Uniformed Services, the Merchant Marine, and the commissioned corps of the Public Health Service and the National Oceanic and Atmospheric Administration, their eligible family members and U.S. citizens residing outside the United States" to vote using absentee ballots.[44]

Vote Centers

Traditionally, voters cast votes at assigned polling places within their specific precinct. Recently, in order to facilitate more efficient voting, numerous states have moved to consolidate voting in vote centers (see Figure 3-6). A vote center serves as a jurisdictional hub where any voter registered in that jurisdiction may vote, regardless of the precinct in which the voter resides.[45] Three states, Wyoming, South Dakota, and Iowa, allow jurisdictions to use vote centers only on Election Day. Twelve states and the District of Columbia allow jurisdictions to use vote centers during early voting only,[46] and eight states allow the use of vote centers during early voting and on Election Day.[47] California has authorized the use of vote centers starting in 2018.[48]

Collection Points for Ballots Received Early

Some jurisdictions provide secure facilities where voters may deposit ballots received early either before or on Election Day.

COUNTING VOTES

Votes are counted in three principal ways: (1) votes cast on paper ballots may be counted manually; (2) paper ballots may be scanned and the votes counted digitally; and (3) votes cast using electronic systems may be

[43] These percentages were calculated using the U.S. Census Bureau's, "Current Population Survey Voting and Registration Supplement," 2016. Utah did not report in the "2016 Election Administration and Voting Survey" (EAVS) the number of ballots cast by mail, which necessitated the use of a survey-based method to estimate vote-by-mail usage.

[44] 52 U.S.C. §§ 20301 *et seq.*

[45] See, for example, Colorado Revised Statutes 1-4-104 (49.8).Georgia, I

[46] The states are Florida, Georgia, llinois, Kansas, Louisiana, Maryland, Massachusetts, Nevada, North Carolina, Ohio, Tennessee, and West Virginia.

[47] The states are Arizona, Arkansas, Colorado, Indiana, New Mexico, North Dakota, Texas, and Utah.

[48] See http://www.ncsl.org/research/elections-and-campaigns/vote-centers.aspx.

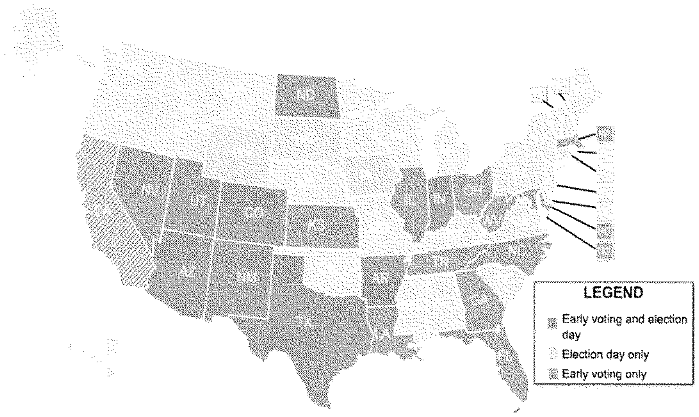


FIGURE 3-6 Vote centers in the United States.
The California Voter's Choice Act allows voters to cast ballots at vote centers in a limited number of counties beginning in 2018. See http://www.sos.ca.gov/elections/voters-choice-act/.
SOURCE: Masterson, Matthew, U.S. Election Assistance Commission, presentation to the committee, April 5, 2017, Washington, DC. The original image, which is available at: http://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_178367.pdf, is the work of the U.S. Election Assistance Commission, taken or made during the course of an employee's official duties. As a work of the U.S. federal government, the image is in the public domain.

counted digitally. In the latter case, a paper ballot is not employed. When paper ballots are scanned, the results are tabulated, and printed, after the close of polls. The scanning may occur in one of two places—in the precinct where the ballots were cast, or in a central counting facility.

At the end of Election Day, if ballots were counted in the precinct, unofficial vote totals are communicated to a central election office through one of several means. These include paper printouts, hand-written paper forms, telephone, modem, and computer memory cards. Either on Election Day or soon thereafter, official returns are most likely to be communicated to the central office by traditional means, e.g., in paper form through the mails or via couriers.

Multiple safeguards are put in place to protect against tampering with vote counts.[49] These safeguards start at the point where the votes are

[49] In many states, safeguards were written into legislation prior to computerization and may not, therefore, offer the protections that they once did.

counted. States generally allow votes to be counted in the presence of the public, although these same laws may give precedence to some parts of the public (such as representatives of political parties) or require that the public be physically distanced from the vote counters. States commonly require that precinct vote returns be posted at the precinct once the counting is finished. This allows the public, candidates, and political parties an opportunity to record a precinct's vote count and subsequently compare it to totals published later.

States have laws that mandate the protection of ballots and other equipment used in elections, in the event a recount is necessary or if a count were to otherwise be called into question.

Ballots received by mail are typically sent directly to the central elections department. Mail-in ballots generally have two envelopes: an inner, plain envelope for the ballot; and an outer envelope with a signature line. The completed ballot is placed in the inner envelope, and the envelope is sealed. This envelope is then placed in the outer envelope, the outer envelope is sealed, and the voter signs on the signature line. When the ballot is received by the elections department, officials ensure that the signature on the outer envelope matches a signature on file with the department. If the signature matches, the inner envelope is removed and placed apart from the outer envelope. The inner envelopes are then opened and counted by an optical-scan reader or other mechanism.

CERTIFYING RESULTS

The tallies reported on election night are not the final results of the election. Instead, the official results of an election are not determined until the election returns have been validated through a process known as canvassing.[50] This validation involves not only rechecking the results reported on election night, but also adjudicating the status of provisional ballots and including ballots that may have arrived by mail after Election Day. Deadlines for the receipt of mail ballots vary by states, with many allowing mail ballots to be counted if they are postmarked before Election Day and arrive within a specified time after Election Day.[51] Once all vote numbers have been reconciled, the local election authority certifies the election for the jurisdiction and generates a report with the official vote count.[52] Results of statewide contests are further certified by state authorities, such as a state

[50] U.S. Election Assistance Commission, "Quickstart Management Guide: Canvassing and Certifying an Election," October 2008, p. 3, available at: https://www.eac.gov/assets/1/6/Quick%20Start-Canvassing%20and%20Certifying%20an%20Election.pdf.

[51] For a list of state deadlines from the 2016 election, see https://web.archive.org/web/20161108023142/https://www.vote.org/absentee-ballot-deadlines/.

[52] Ibid.

elections board. All states have laws that provide mechanisms to contest election results and to recount votes when election results are close.

ELECTION AUDITING

Most local jurisdictions conduct audits after an election, either because auditing is mandated by law or because local officials have independently adopted an audit requirement.[53,54] Some audits scrutinize the processes followed by election officials to ensure that proper procedures were followed. Such audits are referred to as performance audits.

Elections audits also may be conducted to reconcile the record of the number of voters who signed precinct pollbooks with the total number of ballots cast in the precinct and to check that the results of an election are consistent with the physical or electronic record that is produced by voters.

One recently developed class of post-election audits is risk-limiting audits.[55] Risk-limiting audits provide statistical assurance that a reported outcome is the same as the result that would be obtained if all ballots were examined by hand by ensuring that a different reported outcome has a high probability of being detected and corrected. Risk-limiting audits are typically performed by examining a random sample of the cast paper ballots and comparing their contents to expected results. Increasingly, election administrators are looking to risk-limiting audits to help ensure the accuracy and security of the vote and increase confidence in the outcome of elections. In 2018, Colorado will become the first state to conduct risk-limiting audits for a statewide election.[56]

[53] For a discussion of current state post-election audit practices, see, for example, National Conference of State Legislatures, "Post-Election Audits," available at: http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx.

[54] Equipment used in elections may also undergo various forms of testing to attempt to improve integrity and security of election systems. These may include both pre-election and post-election testing of the hardware and software components of election systems. Pre-election testing of voting equipment is referred to as "logic and accuracy testing." Such pre-election testing is conducted primarily as an assurance against non-adversarial errors and breakdowns impacting accuracy.

[55] Philip B. Stark, Associate Dean, Division of Mathematical and Physical Sciences and Professor of Statistics, University of California, Berkeley, invented risk-limiting audits. Jennie Bretschneider, Office of the California Secretary of State; Sean Flaherty, Iowans for Voting Integrity; Susannah Goodman, Common Cause; Mark Halvorson, Citizens for Election Integrity Minnesota; Roger Johnston, Argonne National Laboratory; Mark Lindeman, Columbia University; Ronald L. Rivest, a member of the committee that authored the current report; and Pam Smith, Verified Voting, contributed to the development of Stark's work.

[56] Morrell, Jennifer, Arapahoe County (CO) Elections Director; Hilary Hall, Boulder County (CO) Clerk and Recorder; and Amber McReynolds, Denver (CO) County Elections Director, presentation to committee, December 7, 2017, Denver, CO.

CONCLUSION

For processes from voter registration to the casting and tabulation of votes, election administrators are responsible for the acquisition, maintenance, and oversight of numerous systems that often interact in complex ways. Each system plays an integral part in ensuring that the results of an election are consistent with the will of the voter. In Chapters 4, 5, 6, and 7, the committee provides its analyses of the challenges faced by the nation in achieving accurate elections and offers its recommendations to address these challenges.

4

Analysis of Components of Elections

In this chapter, the committee examines and provides recommendations regarding key components of U.S. elections. The topics discussed are voter registration and voter registration lists, absentee voting, pollbooks, ballot design, voting technology, and voting system certification. Weaknesses in any component can undermine the integrity of elections.

VOTER REGISTRATION AND VOTER REGISTRATION LISTS

Overview and Analysis

Federal and state laws and regulations govern voter eligibility. Federal law, for instance, stipulates that U.S. citizens of at least 18 years of age be entitled to vote in federal elections. State laws require that a voter be a resident (in some cases, resident for some minimum period of time, such as 30 days) of the state. Some states limit voter eligibility on the basis of criminal status or mental competency, although the specifics of such limitations vary. Some communities allow part-time residents who would otherwise be ineligible to vote to cast ballots in local election contests.

Constitutional provisions and federal statutes regulate how states administer voter registration. Since the 1960s, Congress has gradually expanded federal oversight of election administration and registration provisions. The Voting Rights Act (VRA) of 1965 prohibits discriminatory voting practices and prevents an individual from being denied the right to vote because of errors or omissions on registration materials that are not material to determining the voter's qualification to vote. Subsequent legislation aimed at facilitating voter registration includes the Voting Accessibility for the Elderly and Handicapped Act (VAEHA) of 1984 and the Uniformed and Overseas Citizen Absentee Voting Act (UOCAVA) of 1986. The National Voter Registration Act (NVRA) of 1993 requires that applications be made available at a variety of public locations and by mail and establishes broad guidelines concerning the maintenance of voter registration lists.[1]

The 2002 Help America Vote Act (HAVA) requires states to move from locally administered registration lists to state-level centralized, computerized voter registration lists. These state lists act as the official record of eligible voters for federal elections. HAVA requires regular maintenance of the lists for accuracy and completeness and stipulates that state or local officials should provide "adequate technological security measures to prevent the unauthorized access to the computerized" voter registration list.[2] The Act requires that a unique identifier be assigned to each legally registered voter in the state's voter registration list.[3] It states that applications for voter registration may not be accepted or processed by states without either a driver's license number, the last four digits of the applicant's Social Security number, or state-issued identification[4] and requires that those who register by mail present identifying information at the polls on Election Day the first time they vote (or with their mail-in ballots if voting by mail).[5]

An applicant's original signature on a voter registration form constitutes certification that the information provided is true, may be used to authenticate the identity of a voter if there are changes in the registrant's voting status, and often provides a means for authenticating the identity of the voter at a polling place or when processing absentee and/or mailed ballots.

If a voter registers to vote at a department of motor vehicles (DMV), relevant personal information may be provided at the DMV or extracted from the information in DMV files. This information is then transmitted electronically to the relevant election office with a copy of the signature

[1] Voting Accessibility for Elderly and Handicapped Act, 52 U.S.C. §§ 20101 *et seq.*; Uniformed and Overseas Citizens Absentee Voting Act, 52 U.S.C. §§ 20301 *et seq.*; National Voter Registration Act, 52 U.S.C. §§ 20501 *et seq.*

[2] HAVA, § 303.a.3, 52 U.S.C. § 21083. The Act does not specify what measures should be employed.

[3] HAVA, § 303.a.1.A, 52 U.S.C. § 21083.

[4] HAVA, § 303.a.5.A.i.I-II, 52 U.S.C. § 21083. "If an applicant for voter registration for an election for Federal office has not been issued a current and valid driver's license or a Social Security number, the State shall assign the applicant a number which will serve to identify the applicant for voter registration purposes. To the extent that the State has a computerized list in effect under this subsection and the list assigns unique identifying numbers to registrants, the number assigned under this clause shall be the unique identifying number assigned under the list (see Section 303.a.5.A.ii).

[5] HAVA, § 303.b.2.A.i.I-II, 52 U.S.C. § 21083.

on file with the DMV. When voters register entirely online, original signatures on file with DMVs or other agencies may be used for authentication purposes.

In those jurisdictions using the most common form of automatic voter registration, when an individual registers for a driver's license, information is shared with the state elections agency, where eligibility is established and, if eligible, the individual is registered to vote.[6] States have adopted various methods for individuals to opt out of registration, ranging from opting-out at the DMV to being notified of procedures to opt-out via a post card.[7]

Before adding individuals to a voter registration list, an attempt must be made to verify the information provided on a first-time voter registration application against the relevant state's department of motor vehicles database of driver's license numbers or the Social Security Administration's (SSA's) database of Social Security numbers. For a non-match, election administrators in most states will attempt to contact the applicant so that he or she can provide additional information. HAVA requires that an applicant who cannot be matched to a database be allowed to cast a provisional ballot on Election Day "upon the execution of a written affirmation by the individual . . . stating that the individual is . . . a registered voter in the jurisdiction in which the individual desires to vote; and" is "eligible to vote in that election."[8]

Federal law also requires states to establish a program "that makes a reasonable effort to remove the names of ineligible voters" from official voter registration lists.[9] States may use information supplied by the U.S. Postal Service (USPS) to identify registrants whose address may have changed.[10] To identify voters who have moved, election administrators often send periodic mailings to all voters in the jurisdiction or consult third-party move data. The envelope indicates that the mailing should not be forwarded and should be returned to the sender. Notices that are returned to the election official are an indication that the voter may have moved.

The databases containing voter registration lists often are connected, directly or indirectly, to the Internet or state computer networks. This connectivity raises concerns about unauthorized access to or manipulation of the registrant list or disruption of the registration system. Incidents of external intrusions have been reported recently:

[6] Some states have expanded the set of state agencies that can contribute new voters to the rolls, such as social service agencies and Alaska's Permanent Fund Dividend agency.

DMV databases are known to be unreliable.

[7] See National Conference of State Legislatures, "Automatic Voter Registration," available at: http://www.ncsl.org/research/elections-and-campaigns/automatic-voter-registration.aspx.

[8] See HAVA § 302.a, 52 U.S.C. § 21083.

[9] National Voter Registration Act of 1993 (NVRA) § 8.a.4, 52 U.S.C. §§ 20501–20511.

[10] NVRA, § 8.c.A, 52 U.S.C. §§ 20501–20511.

- In Illinois, Russian actors targeted and breached an online voter database in 2016 by exploiting a coding error.[11] For 3 weeks, they maintained undetected access to the system. Ultimately, personal information was obtained on more than 90,000 voters.[12]
- In California, hackers penetrated state registration databases and gained access to the personal information of a large number of voters.[13]
- In Georgia, more than 6.5 million voter records and other privileged information were exposed due to a server error. The security vulnerability had not been addressed 6 months after it was first reported to authorities, even though it could have been used to manipulate the state's election system.[14]

Election administrators usually rely on county or state government information technology (IT) departments to secure voter registration databases. In many cases, voter registration offices and election offices are separate departments in county government. In some cases, such as was the case in the Georgia example above, election data may be housed and managed in non-election offices.

Voter registration lists are used for many purposes other than establishing the eligibility of an individual to vote in an election. Voter registration lists are used, for example, by candidates and political parties to identify and contact potential voters.[15] At the local level, they are used to estimate how many people will vote, which helps guide election administrators as they prepare polling places for Election Day. These lists also are used in

[11] See Edwards, Brad, "Russian Hack into Illinois Election Database Was Worse Than Thought," CBS Chicago, June 13, 2017, available at: http://chicago.cbslocal.com/2017/06/13/russian-hack-into-illinois-election-database-worse-than-thought/; "Illinois Elections Board Offers More Information on Hacking Incident," WSIU, May 4, 2017, available at: http://news.wsiu.org/post/illinois-elections-board-offers-more-information-hacking-incident#stream/0; and Uchill, Joe, "Illinois Voting Records Hack Didn't Target Specific Records, Says IT Staff," *The Hill*, May 4, 2017, available at: http://thehill.com/policy/cybersecurity/331981-ill-voting-records-hack-didnt-target-specific-records-says-state-it.

[12] "Illinois Elections Board Offers More Information on Hacking Incident."

[13] See Reilly, Katie, "Russians Hacked Arizona Voter Registration Database—Official," *Time*, August 30, 2016, available at: http://time.com/4472169/russian-hackers-arizona-voter-registration/ and Uchill, Joe, "Hackers Demand Ransom for California Voter Database," *The Hill*, December 15, 2017, available at: http://thehill.com/policy/cybersecurity/365113-hackers-demand-ransom-for-california-voter-database.

[14] See Bajak, Frank, "APNewsBreak: Georgia Election Server Wiped After Suit Filed," Associated Press, October 27, 2017, available at: https://www.apnews.com/877ee1015f1c43f1965f63538b035d3f.

[15] See Hersh, Eitan, *Hacking the Electorate: How Campaigns Perceive Voters* (New York: Cambridge University Press, 2015).

some jurisdictions to establish signature and vote thresholds for petitions and referenda and to select jury pools.

Ideally, voter registration lists should include all eligible individuals who wish to be registered and no ineligible individuals. Voter registration lists should, therefore, be both accurate and complete. In this case, the term "accurate" can refer either to the factual correctness of the data that exist in the database or to the notion that the database contains none of the individuals not eligible to vote. The term "complete" refers to the presence in the database of all eligible individuals who wish to be registered.[16]

Maintenance of a voter registration list requires maintaining the currency of the registrant list and removing duplicate registrations and ineligible voters. This task requires comparing records within a voter registration list to other records to identify duplicate registrations (which are usually associated with changes of address or name) and comparing voter registration lists to other official lists that contain information about individuals who are ineligible to vote in a state, typically felons and individuals declared mentally incompetent.[17] Voter lists, of course, must be regularly compared against death registries. Data matching can draw either on intrastate sources, such as social service, motor vehicle, and death records or on interstate sources, such as the cross-state record matching performed by organizations such as the Electronic Registration Information Center (ERIC) and the Interstate Voter Registration Crosscheck System.[18,19,20] HAVA provides some criteria for developing and maintaining voter registration databases, and the U.S. Election Assistance Commission (EAC)

[16] See National Research Council, *Improving State Voter Registration Databases: Final Report*, (Washington, DC: The National Academies Press, 2010), available at: https://doi.org/10.17226/12788, p. 2.

[17] Ibid, p. 1.

[18] Data matching systems are imperfect. They can—and do—generate false matches that could potentially lead to the disenfranchisement of legitimate voters.

[19] ERIC "is a non-profit organization with the sole mission of assisting states to improve the accuracy of America's voter rolls and increase access to voter registration for all eligible citizens" (see http://www.ericstates.org/). As of the writing of this report, 22 states and the District of Columbia are members of ERIC. The 22 states are Alabama, Alaska, Arizona, Colorado, Connecticut, Delaware, Louisiana, Illinois, Maryland, Minnesota, Missouri, Nevada, New Mexico, Ohio, Oregon, Pennsylvania, Rhode Island, Utah, Virginia, Washington, West Virginia, and Wisconsin. See http://www.ericstates.org/faq.

[20] The Interstate Voter Registration Crosscheck System is operated by the office of the Secretary of State of the state of Kansas. The system compares voter rolls in participating states to identify potential duplicate voter registrations. It identifies voter registrations that have identical first names, last names, and dates of birth. According to the office of the Kansas Secretary of State, 28 states participated in Crosscheck in 2017. See http://www.wbur.org/radioboston/2017/11/03/massachusetts-crosscheck-system.

The system recently halted operations due to accuracy and security concerns raised by the U.S. Department of Homeland Security.

has issued guidance, but states maintain a degree of discretion in how to conform to these requirements.[21]

States have taken different approaches to building systems to meet the federal requirement for centralized voter registration lists. Under the so-called "top-down" approach followed by many states, state election administrators maintain a single, unified database and local election administrators provide the state with updates for the information needed in the database. Some states have instead opted for a bottom-up approach. In this scenario, local jurisdictions maintain their own registration lists but provide periodic updates to a separate statewide system. Other states use a hybrid approach that combines elements of both the top-down and bottom-up approaches.

The EAC's "2016 Statutory Overview" found that 38 states have voter registration databases that use a top-down approach, 9 have a hybrid system where counties manage their voter registration databases either through direct use of the state's database or independently using a third-party vendor (in the latter case, data is uploaded nightly to the state database), and 6 states employ a bottom-up approach.[22]

The USPS does not automatically notify election administrators of an individual's change of address. Election administrators must initiate address checks with USPS on their own. States may also obtain information on changes of address from departments of motor vehicles or other state agencies.

Two recent court decisions have significant implications for voter registration. In *Fish v. Kobach*, voters sued Kansas Secretary of State Kris Kobach for enforcing a state law that required Kansans to provide proof-of-citizenship documents in order to register to vote.[23] On June 18, 2018, the United States District Court for the District of Kansas found the law to be unconstitutional, because it created an unnecessary burden on voters. In *Husted v. A. Philip Randolph Institute*, the U.S. Supreme Court on June 11, 2018 upheld an Ohio law that allows the state to strike voters from the registration rolls if they fail to return a mailed address confirmation form and then do not vote for 4 years or two federal election cycles.[24] Lower courts had ruled that the law violated the National Voter Registration Act, which states that individuals may not be purged from the voter rolls because of a

[21] See HAVA, Section 303 and U.S. Election Assistance Commission, "Checklist for Securing Voter Registration Data," October 23, 2017, available at: https://www.eac.gov/documents/2017/10/23/checklist-for-securing-voter-registration-data/.

[22] See Green, Seth, "Statewide Voter Registration Systems," August 31, 2017, available at: https://www.eac.gov/statewide-voter-registration-systems/. A table that shows the approach employed by each state is available at this site.

[23] *Fish v. Kobach*, 2:16-cv-02105-JAR (D. Kan. 2018).

[24] *Husted v. A. Philip Randolph Institute,* 584 U.S. ___ (2018).

failure to vote. The Supreme Court concluded that the Ohio law does not deregister voters solely because of a failure to vote, but does so in conjunction with a failure to return an address confirmation form.

States have adopted numerous methods to facilitate voter registration: in person; by mail or fax; Internet; automatic registration; same-day registration. Each have advantages and disadvantages. Automatic voter registration may improve voter participation, reduce costs, and increase the accuracy of voter rolls. It may, however, needlessly register individuals who do not care to be registered, and if the systems are not well designed, it may be possible for noncitizens to end up on the voter rolls.[25] With regard to online registration, cost savings and voter convenience may be benefits. Security risks are, however, an inherent part of any online system.[26] For same-day registration, additional costs may be associated with system implementation (e.g., necessity to purchase additional equipment like e-pollbooks or ballot-on demand printers; costs of network connectivity; costs of updating voter registration systems to accommodate same-day registration, etc.). Some have suggested that same-day registration may increase voter turnout.[27]

Voter rolls inherently contain inaccuracies. Database maintenance is critical, but cannot yield perfect accuracy or completeness. It can be difficult to maintain the accuracy of voter registration lists due to changes in address, name, or life status. Sophisticated tools used in other industries may provide better record matching.[28] ERIC is one organization that attempts to make high-quality industry matching tools available to state election officials, but the existence of ERIC does not preclude states from exploring other record matching tools.

Electronic voter registration databases, like all electronic systems, are vulnerable to cyberattacks. If the contents of a voter registration database are altered or connectivity to a voter registration database is interrupted on Election Day either because of connectivity issues or because of efforts by external actors (e.g., by a denial-of-service attack), the consequences for voter convenience, voter confidence, and elections outcomes could be

[25] See http://www.ncsl.org/research/elections-and-campaigns/automatic-voter-registration.aspx.

[26] See http://www.ncsl.org/research/elections-and-campaigns/electronic-or-online-voter-registration.aspx.

[27] See http://www.ncsl.org/research/elections-and-campaigns/same-day-registration.aspx.

[28] For example: techniques for record linkage; the use of preprocessing to standardize data elements; accounting for the relative frequency of occurrence of values of strings such as first and last names; estimation of optimal matching parameters; and providing methods for estimating false match rates. See National Research Council, *Improving State Voter Registration Databases: Final Report* (Washington, DC: The National Academies Press, 2010), pp. 72-73, available at: https://doi.org/10.17226/12788.

very serious, especially if network-connected e-pollbooks are used and no backup of a voter registration list is available. Even if a voter registration database is not altered, the theft of the information contained in voter registration databases could cause serious problems. Driver's license numbers and Social Security numbers, for example, could be used for identity theft or for the purpose of requesting absentee ballots.[29] Attacks that alter voter registration data could be used to introduce fake or illegitimate voters, to remove valid voters from voter registration databases, or to force provisional voting on Election Day. The latter would likely be detected but could, nevertheless, cause long lines and other disruptions at polling sites. If an attacker targeted voters in jurisdictions that tend to favor one political party, such an attack could have a partisan effect on election results.

Even when a registration database is reasonably protected, online portals that allow voters to update their registration information can provide a point of entry for the alteration of data. Update requests often require weak authentication. In some states, the information required to change a registration is available from public records.

Findings

Simple voter registration methods encourage voter participation. Cumbersome voting registration systems may disenfranchise voters.

Voter registration databases face accuracy and completeness requirements that are in tension with one another. Measures to increase accuracy (e.g., purging suspect data) may reduce completeness. Measures to increase completeness (e.g., not purging suspect data) may reduce accuracy.

Electronic voter registration systems may make it easier to manage and maintain voter registration databases. The use of electronic information from other government sources may increase the accuracy and completeness of the databases.

Electronic voter databases are subject to cybersecurity vulnerabilities and attacks.

Election officials may not have the authority to request or insist on cybersecurity protections for voter registration databases or the resources to pay for appropriate cybersecurity measures.

Voter records contain personally identifiable information that, if compromised, could be used to the detriment of voters outside of the election context.

[29] Only a small number of states are permitted to collect Social Security numbers for voter registration purposes, although all states can collect the last four digits of Social Security numbers.

RECOMMENDATIONS

4.1 Election administrators should routinely assess the integrity of voter registration databases and the integrity of voter registration databases connected to other applications. They should develop plans that detail security procedures for assessing voter registration database integrity and put in place systems that detect efforts to probe, tamper with, or interfere with voter registration systems. States should require election administrators to report any detected compromises or vulnerabilities in voter registration systems to the U.S. Department of Homeland Security, the U.S. Election Assistance Commission, and state officials.

4.2 Vendors should be required to report to their customers, the U.S. Department of Homeland Security, the U.S. Election Assistance Commission, and state officials any detected efforts to probe, tamper with, or interfere with voter registration systems.

4.3 All states should participate in a system of cross-state matching of voter registrations, such as the Electronic Registration Information Center (ERIC). States must ensure that, in the utilization of cross-matching voter databases, eligible voters are not removed from voter rolls.

4.4 Organizations engaged in managing and cross-matching voter information should continue to improve security and privacy practices. These organizations should be subject to external audits to ensure compliance with best security practices.

VOTING BY MAIL, INCLUDING ABSENTEE VOTING

Overview and Analysis

Absentee voting (voting remotely) provides an opportunity to cast a vote by obtaining a ballot (usually a printed ballot obtained by mail) in advance of an election and returning the completed ballot to elections officials by mail[30] or other means. If paper ballots are used, voters typically mark the received ballot and place it in a secrecy envelope or sleeve. The envelope/sleeve is then placed into a second mailing envelope. The voter seals the mailing envelope and signs an affidavit on the envelope's exterior. The ballot is then mailed to the appropriate elections office or deposited at a designated dropoff location.[31] To be counted, absentee ballots must be postmarked, deposited, or received by a deadline that is generally estab-

[30] In at least 22 states, certain elections may be conducted entirely by mail. See http://www.ncsl.org/research/elections-and-campaigns/all-mail-elections.aspx.

[31] See http://www.ncsl.org/research/elections-and-campaigns/all-mail-elections.aspx.

lished by state governments. In many jurisdictions, the identity of the voter is confirmed by matching the signature on the envelope against the signature in the voter registration database.[32]

As discussed in Chapter 3, three states, Washington, Oregon, and Colorado principally use the mails to distribute ballots to all registered voters, and two others, California and Utah, are moving toward this model.[33] In these instances, ballots are mailed to all registered voters. Other "states permit all-mail elections in certain circumstances, such as special districts, municipal elections, when candidates are unopposed, or at the discretion of the county clerk."[34]

In some jurisdictions, signature matching is completed automatically by a computer that compares the signature on a scanned paper ballot to signatures on file in a database. In other jurisdictions, a non-expert election administrator compares signatures. Both methods can result in mismatching. In addition, an individual's signature may change over time. If a signature database is not updated regularly, mismatching may occur. Inaccurate matching may result in the rejection of valid ballots.

Ninety-nine percent of absentee ballots categorized as "returned and submitted for counting" were ultimately counted in the 2016 federal election.[35] In 2016, the most common reasons that absentee ballots were rejected were that the signature on the ballot did not match the signature in a state's records, that the required signature was missing, or that the ballot was received after deadline.[36]

UOCAVA allows "U.S. citizens who are active members of the Uniformed Services, the Merchant Marine, and the commissioned corps of the Public Health Service and the National Oceanic and Atmospheric Administration, their eligible family members and U.S. citizens residing outside

[32] Some states accommodate remote accessible ballot marking. In such states, a voter retrieves and marks a ballot online, prints out the completed ballot, and mails the ballot to the appropriate elections office. See, e.g., https://nfb.org/ohio-requires-accessible-absentee-ballots-blind; https://www.sos.state.oh.us/globalassets/elections/directives/2018/dir2018-03.pdf; https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB2252; and http://sfgov.org/elections/remote-accessible-vote-mail-system.

[33] Masterson, Matthew, U.S. Election Assistance Commission, presentation to the committee, April 5, 2017, Washington, DC. See also "2016 Election Administration and Voting Survey" (EAVS), p. 9.

In Washington, every county has at least one vote center for in-person voting (see https://www.sos.wa.gov/elections/faq_vote_by_mail.aspx). In Oregon, each county elections office provides privacy booths for voters who want to vote in person or voters who need assistance (see https://multco.us/file/31968/download). In Colorado, voters have the option to vote in person at a county Voter Service and Polling Center (VSPC) (see https://www.sos.state.co.us/pubs/elections/FAQs/ElectionDay.html).

[34] See http://www.ncsl.org/research/elections-and-campaigns/all-mail-elections.aspx.

[35] "2016 Election Administration and Voting Survey" (EAVS), p. 10.

[36] Ibid.

the United States" to vote using absentee ballots.[37] UOCAVA voters must have a legal voting residence in the jurisdiction where they want to vote.[38] The USPS and the Military Postal Service Agency (MPSA) have special procedures for handling UOCAVA outgoing and incoming ballots.[39]

In 2009, Congress amended portions of UOCAVA with the Military and Oversees Voter Empowerment Act (MOVE). MOVE stipulates that ballots requested by UOCAVA voters must be transmitted 45 days before a federal election, that voters have the right to receive their ballots by at least one electronic method (email, online, or fax) *or* by mail, and that states must have a system in place to determine whether a ballot was received by the appropriate elections office.[40]

To be counted, UOCAVA ballots must be returned to the appropriate election office before a state-mandated deadline.[41] In 2016, states reported transmitting 930,156 UOCAVA ballots. Of this number, 633,592 were returned.[42] Approximately 110,000 more ballots were transmitted to overseas citizens than to uniformed services voters.[43] Of the UOCAVA ballots returned by voters, 512,696 (80.9 percent) were counted.[44]

Absentee voting introduces benefits and risks that are different from the benefits and risks of in-person voting.[45] By-mail voting increases convenience, especially for the disabled community, and may improve the amount of thought that goes into marking a ballot. A common justification for voting by mail is increasing the amount of deliberation voters give to their ballots. However, the evidence presented to support this claim tends to be anecdotal or based on appeals to logic. There appears to be no peer-reviewed empirical research to quantify the degree to which increased voter knowledge or deliberation is associated with expanding mail-ballot opportunities. There is evidence, though, that the convenience of by-mail voting

[37] See https://www.fvap.gov/info/laws/uocava.

[38] See U.S. Election Assistance Commission, "Tips for Helping UOCAVA Voters and their Families," p. 3, available at: https://www.eac.gov/documents/2017/08/03/six-tips-for-helping-uocava-voters-and-their-families-from-eac-contingency-plan-election-administration-pre-election-security/.

[39] Ibid, p. 6.

[40] Ibid, p. 2.

[41] Ibid, p. 12.

[42] Ibid.

[43] Ibid, p. 11.

[44] Ibid, p. 12.

[45] Stewart, Charles III, "Losing Votes by Mail," *New York University Journal of Legislation and Public Policy 13*, 2010, No. 3, pp. 573-601. Dr. Stewart is a member of the committee that authored the current report.

may stimulate increased voter turnout in certain situations.[46] There are other indications, however, that by-mail voting may initially increase voter turnout rates but that rates then revert to previous turnout patterns and that by-mail voting can depress turnout in presidential and gubernatorial general elections.[47] Further, all-mail voting may produce a cost savings.[48] For instance, in a study of Colorado's 2013 mandate that mail ballots be sent to all registered voters, the Pew Charitable Trusts estimated that this reform decreased costs by an average of 40 percent, in addition to reducing the use of provisional ballots by 98 percent.[49]

Remote voting creates new opportunities for coercion and for loss of privacy that in-person voting attempts to overcome.[50] Outside of the privacy of a voting booth, other individuals may buy or sell votes or overtly pressure a voter to make particular ballot selections. Ballots may be stolen or intercepted by third parties who mark and cast them. It may also be easier for an election administrator to examine a ballot before it is separated from its identifying outer envelope or email header. In the case of all-mail voting, the dependence on written instructions rather than poll-worker assistance may disadvantage some voters and increase the residual vote rate.[51]

The paths that mail ballots travel introduce other risks that are typically avoided with in-person voting. Most absentee and mail balloting relies on the U.S. postal system to (1) deliver the request for an absentee ballot from the voter to the local jurisdiction; (2) deliver the unmarked ballot from

[46] See Gerber, Alan S., Gregory A. Huber, and Seth J. Hill, "Identifying the Effect of All-mail Elections on Turnout: Staggered Reform in the Evergreen State," *Political Science Research and Methods*, 2013, Vol. 1, No. 1, pp. 91-116; Miller, Peter and Sierra Powell, "Overcoming Voting Obstacles: The Use of Convenience Voting by Voters with Disabilities," *American Politics Research*, 2016, Vol 44, No. 1, pp. 28-55; and Flaxman, Seth, Marie-Fatima Hyacinthe, Parker Lawson, and Kathryn Peters," Voting by Mail: Increasing the Use and Reliability of Mail-Based Voting Options," available at: http://web.mit.edu/supportthevoter/www/files/2013/11/Vote-by-Mail-Reform-Memo.pdf.

[47] See, e.g., https://www.eac.gov/documents/2017/02/23/will-vote-by-mail-elections-increase-turnout/.

[48] See "Voting by Mail: Increasing the Use and Reliability of Mail-Based Voting Options."

[49] Pew Charitable Trusts, "Colorado Voting Reforms: Early Results," available at: http://www.pewtrusts.org/-/media/assets/2016/03/coloradovotingreformsearlyresults.pdf.

[50] See http://www.ncsl.org/research/elections-and-campaigns/all-mail-elections.aspx.

[51] Alvarez, R. Michael, Dustin Beckett, and Charles Stewart III, "Voting Technology, Vote-by-Mail, and Residual Votes in California, 1990–2010," *Political Research Quarterly*, 2013, Vol. 66, No. 3, pp. 658-670.

"Residual votes" are the sum of over- and under-votes on a ballot, typically measured at the top of the ticket. See Stewart, Charles III, "Voting Technologies," *Annual Review of Political Science*, 2011, Vol. 14, pp. 353-378. Dr. Stewart is a member of the committee that authored the current report.

the jurisdiction back to the voter; and (3) deliver the marked ballot back to the election jurisdiction for counting.

The marked ballot is a more valuable target than a request for a mail ballot or even the unmarked ballot. The secrecy associated with marked ballots makes it more difficult for a voter to detect whether a marked ballot has been tampered with or intercepted.

The heavy reliance on the U.S. postal system for mail ballots introduces potential problems related to inconsistencies in service. "Mail delivery is not uniform across the nation. Native Americans on reservations may in particular have difficulty. Many do not have street addresses, and their P.O. boxes may be shared."[52] The mail return of marked ballots may be delayed past the deadline. Since, currently, there are no agreed upon chain-of-custody procedures for mailed ballots, mail-in voting presents more chances for votes to be lost than is the case with in-person voting. Collection points for mail-in ballots reduce dependence on the postal system and provide voters with greater assurance that their ballots will be received.[53]

Because of concerns about the chain-of-custody of mail ballots, local election officials—often in direct cooperation with the USPS—have adopted practices to allow officials and voters to track the location of mail ballots through the mail stream.[54] These systems allow postal mail to be tracked via the USPS's Intelligent Mail Barcode. There are services available to election officials to facilitate the use of this data, including products like Ballot Scout, Ballot Tracks, and Ballot Trace.[55]

Concerns over the speed and reliability of the USPS have led to the replacement of the mails with electronic means, particularly the Internet, in the administration of voting by mail in many jurisdictions. While there are administrative gains to be had by moving to the electronic transmission of absentee ballot requests, and the transmission of unmarked ballots to voters, this practice comes with many of the cybersecurity vulnerabilities discussed in Chapter 5 of this report. However, because there are also vulnerabilities with using the mails to request absentee ballots and transmit unmarked ballots to voters, it may be that relying on the Internet for these portions of the vote-by-mail system could lead to a net improvement

[52] See http://www.ncsl.org/research/elections-and-campaigns/all-mail-elections.aspx.

[53] Stewart, Charles III, "Losing Votes by Mail," *Journal of Legislation and Public Policy*, Vol. 13, No. 3, pp. 573-601. Dr. Stewart is a member of the committee that authored the current report.

[54] Bipartisan Policy Center, "The New Realities of Voting by Mail in 2016," June 2016, available at: https://bipartisanpolicy.org/wp-content/uploads/2016/06/BPC-Voting-By-Mail.pdf.

[55] In the 2014 federal election, 35 states had tools on their state election websites that allowed voters to track their absentee ballots. See Pew Charitable Trusts, "Elections Performance Index," available at: http://www.pewtrusts.org/en/multimedia/data-visualizations/2014/elections-performance-index#indicatorProfile-OLT.

in the administration of mail-balloting. However, it appears that no peer-reviewed research has comprehensively assessed the relative risk-reward tradeoffs involved in using the mails to transmit absentee ballot requests and unmarked ballots.

Few marked ballots are currently transmitted electronically. The electronic transmission of absentee ballots—via fax, email, or web portal—is most often reserved for voters who fall under UOCAVA "as these voters often face unique challenges in obtaining and returning absentee ballots within state deadlines."[56] Three states, Arizona, Missouri, and North Dakota, allow some voters to return marked ballots using a web-based portal, but Missouri only offers electronic ballot return for military voters serving in a "hostile zone."[57] In North Dakota and Arizona, any UOCAVA voter may use the web option.[58] The singular importance of the marked ballot may help explain why few marked ballots are currently transmitted electronically.

Findings

Vote-by-mail may increase convenience and satisfaction, as voters may complete ballots from the comfort of their home and devote as much time as they wish to assess candidates and issues.

Vote-by-mail can make voting more accessible for individuals with disabilities.

[56] See http://www.ncsl.org/research/elections-and-campaigns/Internet-voting.aspx.

[57] "Alabama conducted a pilot project in 2016 to permit UOCAVA voters located outside of U.S. territorial limits to submit voted ballots via a web portal, but the state has not made this program permanent. Alaska previously made a web portal available to any absentee voter to return a voted ballot, but discontinued this option in 2018." See http://www.ncsl.org/research/elections-and-campaigns/Internet-voting.aspx.

The state of Washington allows all voters to return ballots as email attachments—although non-UOCAVA voters must follow up with a physical ballot to have their electronic ballots counted.

The West Virginia Secretary of State has recently announced a pilot to offer voting via mobile devices to military voters. See https://sos.wv.gov/News-Center/Pages/Military-Mobile-Voting-Pilot-Project.aspx.

[58] See http://www.ncsl.org/research/elections-and-campaigns/Internet-voting.aspx.

Twenty-one states (Colorado, Delaware, Hawaii, Idaho, Indiana, Iowa, Kansas, Maine, Massachusetts, Mississippi, Montana, Nebraska, Nevada, New Jersey, New Mexico, North Carolina, Oregon, South Carolina, Utah, Washington, and West Virginia) and the District of Columbia allow some voters to return ballots via email or fax.

Seven states (Alaska, California, Florida, Louisiana, Oklahoma, Rhode Island, and Texas) allow some voters to return ballots via fax.

Nineteen states (Alabama, Arkansas, Connecticut, Georgia, Illinois, Kentucky, Maryland, Michigan, Minnesota, New Hampshire, New York, Ohio, Pennsylvania, South Dakota, Tennessee, Vermont, Virginia, Wisconsin, and Wyoming) do not allow electronic return of ballots. Voters must return voted ballots via postal mail. See http://www.ncsl.org/research/elections-and-campaigns/Internet-voting.aspx.

Vote-by-mail may produce cost savings.

Vote-by mail requires careful design of ballot transmittal envelopes and tabulation procedures.

With vote-by-mail, it is not possible to guarantee that a voter has cast his or her ballot privately. A voter might be coerced into making particular selections.

Currently, there are no agreed upon chain-of-custody procedures for mailed ballots. Vote-by-mail presents more chances for votes to be lost than is the case with in-person voting.

Drop boxes for mail-in ballots outside of elections offices reduce dependence on the postal system.

Collection points for mail-in ballots introduce additional points of failure and security concerns.

Election jurisdictions are increasingly adopting programs that allow officials and voters to track the location of mail ballots.

All-mail elections may slow down the vote counting process, especially if ballots are accepted according to postmark date (and thus may be received and counted days or weeks after the election).

UOCAVA voting presents unique challenges for election administration with regard to the transmission of ballots to and from remote locations.

RECOMMENDATION

4.5 All voting jurisdictions should provide means for a voter to easily check whether a ballot sent by mail has been dispatched to him or her and, subsequently, whether his or her marked ballot has been received and accepted by the appropriate elections officials.

POLLBOOKS

Overview and Analysis

When a voter arrives at a polling place, the voter typically "checks in" to vote by providing a name and/or some form of identification to a poll worker, who matches the given name to information in a pollbook.[59] In some states, voters may be required to fulfill a non-documentary identification requirement. In lieu of presenting a document that establishes their identity, they might, for instance, be required to sign an affidavit asserting eligibility to vote, provide a signature, or provide personal information either orally or in writing. Once an individual's eligibility to vote has been

[59] Thirty-four states have laws requesting or requiring voters to show some sort of identification at the polls. See http://www.ncsl.org/research/elections-and-campaigns/voter-id.aspx.

determined, an eligible voter may proceed to cast a vote. If an individual's eligibility cannot be confirmed, that individual must be offered the opportunity to cast a provisional ballot. The procedures for when to issue and count provisional ballots are established by individual states.[60]

While most jurisdictions (81.8 percent) still use preprinted paper registration lists to check in voters, between the 2012 to 2016 federal elections, there was a 75 percent increase in the use of electronic pollbooks (e-pollbooks) where paper is replaced by computers either containing locally stored lists of registered voters or connected to digital voter registration databases via the Internet. In the 2016 election, at least 1,146 jurisdictions (17.7 percent of all jurisdictions) used e-pollbooks.[61] Because larger jurisdictions tend to use e-pollbooks, the fraction of voters checked-in using e-pollbooks is close to 50 percent.[62]

E-pollbooks provide more data to poll workers than traditional paper pollbooks. E-pollbooks may be networked and receive immediate updates on who has voted in other voting locations. They may allow poll workers to look up voters from an entire county or state or notify a poll worker that a voter has already voted.[63] A poll worker may use an e-pollbook to direct a voter to the correct polling location. E-pollbooks may also host on-demand training tips and procedural guides for poll workers. "Some e-pollbooks can scan driver's licenses, speeding up the voter check-in process. Other e-pollbooks use an electronic signature pad that immediately captures the voter's signature."[64] E-pollbooks may also produce turnout numbers and lists of those who voted.[65]

The requirements for the certification of e-pollbooks vary considerably among the states and jurisdictions that permit their use.[66] As of March 2017, only eight states certify e-pollbooks. Eleven states have statutes

[60] See Appendix E.

[61] "2016 Election Administration and Voting Survey" (EAVS), p. 8.

[62] This figure was calculated directly from the Election Administration and Voting Survey dataset available on the website of the U.S. Election Assistance Commission at https://www.eac.gov/research-and-data/election-administration-voting-survey/.

[63] With regard to absentee ballots, standard practice is to check voter registration systems to see whether the voter is recorded as having already voted. If an individual has returned an absentee ballot prior to Election Day, this information should be reflected in the poll book (whether it is electronic or not). If the absentee ballot arrives after Election Day and the voter cast a ballot on Election Day, the absentee ballot should be reflected in the voter registration system. The issue of multiple voting is most critical in jurisdictions with multiple vote centers. In this instance, it is important that e-pollbooks be updated in real time.

[64] See Hubler, Katie Owens, "All About E-Poll Books," *NCSL's The Canvass*, Issue 46, February 2014, available at: http://www.ncsl.org/research/elections-and-campaigns/the-canvass-february-2014.aspx#Poll%20Books.

[65] Ibid.

[66] In general, to achieve certification, a system must undergo independent testing to verify that it meets specified requirements for design and performance.

explicitly authorizing the use of e-pollbooks, three states have statutes referring to e-pollbooks without explicitly authorizing their use, five states have established procedures or certification requirements dictated by the state but not by statute, and three states have jurisdictions that used e-pollbooks absent mention in statute or rule.[67]

While attacks on e-pollbooks could be used to change voter data, prevent access to voter registration data, fool the devices' check-in logic to allow multiple voting by individuals, or access back-end systems, there are no national security standards for e-pollbooks.[68] As a result, security practices vary across states. Some states conduct testing before each election, some make backup e-pollbooks available on Election Day, and some make backup paper rolls available on Election Day. Others leave testing or audits up to individual counties or provide no backup system.[69]

The static nature of printed pollbooks presents several problems, because voter registration recruitment continues until the registration deadline.[70] Voter registration offices may not be able to finish entering registrant data into voter registration databases before pollbooks must be printed for distribution to polling places. In light of this, some voter registration offices create supplemental lists for distribution to election judges immediately prior to an election. The success of this approach depends on numerous logistical factors (e.g., timely delivery).

Paper pollbooks may present a risk in the context of convenience programs like vote centers and early voting, as the use of paper pollbooks would not prevent a voter from casting a ballot in more than one location. In such scenarios, multiple voting may only become apparent after the fact, and documentation may not be enough for successful prosecution. While voter registration offices may be contacted to qualify each voter, voter registration call centers have limited capacity, and cell phone service at polling places may not be reliable.

Provided that they are properly counted, the use of provisional ballots offers a potential solution to a compromised e-pollbook system. However, if an e-pollbook system were compromised to the point that a jurisdiction had to rely solely on provisional ballots, it is likely that the delays produced by the provisional ballot procedure, and the attending chaos at

[67] See http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx.

[68] See Norden, Lawrence and Ian Vandewalker, Brennan Center for Justice, "Securing Elections from Foreign Interference," 2017, available at: https://www.brennancenter.org/sites/default/files/publications/Securing_Elections_From_Foreign_Interference_1.pdf.

[69] See Pew Charitable Trust, "A Look at How—and How Many—States Adopt Electronic Poll Books," available at: http://www.pewtrusts.org/en/multimedia/data-visualizations/2017/a-look-at-how-and-how-many-states-adopt-electronic-poll-books.

[70] The move in many jurisdictions to same-day registration means that the contents of pollbooks may be in flux even on Election Day.

the polls, would produce significant problems with voter confidence—and perhaps disenfranchise voters. Nonetheless, if paper poll books are used in emergencies, it will be possible to determine the number of illegal multiple votes after the election ends. This acts not only as a deterrent to unlawful voting but as a mechanism for determining whether illegal votes may have changed the outcome of an election.

The move in many jurisdictions to same-day registration and early voting makes it necessary to provide distributed access to pollbooks and real-time information on those who are registered to vote or who have voted. This reliance on connectivity presents cybersecurity risks.

E-pollbooks help to ensure that an individual casts only a single ballot as they are able to offer, through online connectivity, access to the most current version of the voter registration database. Voter registration offices can focus on data entry through the early voting period—and even up to Election Day—since data entry need not be completed to meet the cut-off time for the printing and delivery of paper pollbooks.

Findings

Eligible voters may be denied the opportunity to vote a regular ballot if pollbooks are inaccurate.

Internet access to e-pollbooks increases the risks associated with the use of e-pollbooks to manage elections. Cyberattacks can alter the voter registration databases used to generate and update pollbooks. If pollbooks are altered by external actors, eligible citizens might, on election days, be denied the right to vote or ineligible individuals might be permitted to vote. Cyberattacks could also compromise the record of who actually voted on Election Day—or disrupt an election in numerous other ways.

If an e-pollbook is connected to a remote voter registration database and there is no offline backup, a denial-of-service cyberattack could force voting to be halted.

Cybersecurity risks are a factor for consideration when making the decision to use Internet-connected e-pollbooks.

RECOMMENDATIONS

4.6 Jurisdictions that use electronic pollbooks should have backup plans in place to provide access to current voter registration lists in the event of any disruption.

4.7 Congress should authorize and fund the National Institute of Standards and Technology, in consultation with the U.S. Election Assistance Commission, to develop security standards and verification and validation protocols for electronic pollbooks in

addition to the standards and verification and validation protocols they have developed for voting systems.

4.8 **Election administrators should routinely assess the security of electronic pollbooks against a range of threats such as threats to the integrity, confidentiality, or availability of pollbooks. They should develop plans that detail security procedures for assessing electronic pollbook integrity.**

BALLOT DESIGN

Overview and Analysis

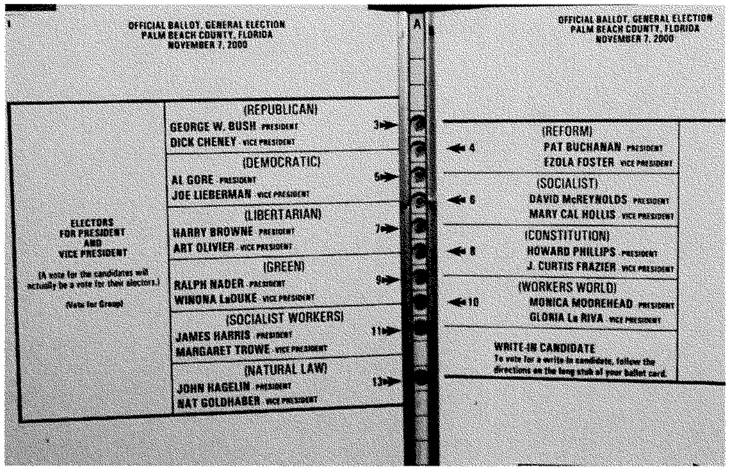
The visual presentation of information on ballots has long been a topic of study. With regard to the presentation of information to voters, confidence in the outcome of elections is enhanced when ballots present information clearly and allow voters to make their selections in an intuitive way. Poor ballot design causes confusion and increases the possibility of a cast vote not reflecting the intention of the voter. Poor design may therefore threaten the accuracy of election results, since it may result in votes not cast as intended.

Ballot design requirements are often dictated by state law. Some states legislate the precise language that must be used on a ballot, and sometimes the exact design as well (e.g., layout or font size), making it difficult to update language or improve the functionality of the ballot over time. While there are some benefits to this prescriptive approach, it can hamper the implementation of new technology and introduce confusion for voters.

Ballot designs vary widely and depend on the voting machine or technology in use. Ballots can look different on different machines. Some ballots, like California's, are typically very long because they may include many statewide offices and initiatives. Initiatives are accompanied by short explanatory text which further extends the length of the ballot.

Poor ballot design can occur when election administrators fail to incorporate proven design principles or are constrained from doing so by voting technology features or local laws and regulations. Problems arise when a typeface is too small, the layout of the ballot is confusing, or the proper place or method to mark the voter's choice is difficult to discern. Poor ballot design has led to overvoting (inadvertently voting for more than one candidate for the same office), undervoting (failing to vote for any candidate in a contest), and mistaken selections. If, in the latter case, a voter attempts to strike out the erroneous vote and indicate an alternate choice, the ballot may be spoiled.

Two well-known examples of poor ballot design originated in Florida. The Palm Beach County "butterfly ballot" (see Figure 4-1) from the 2000 presidential election provides an example of how confusing ballot design can lead to miscast votes. The two-page ballot presented candidate names staggered on alternate sides of a central punch button column. The design directly contributed to an increased number of miscast votes in the election.[71] The 2006 general election ballot from Sarasota County illustrates how poor electronic ballot design (see Figure 4-2) may have caused many voters to overlook a congressional race.



1

OFFICIAL BALLOT, GENERAL ELECTION
PALM BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000

ELECTORS
FOR PRESIDENT
AND
VICE PRESIDENT

(A vote for the candidates will actually be a vote for their electors.)

(Vote for Group)

(REPUBLICAN)
GEORGE W. BUSH PRESIDENT
DICK CHENEY VICE PRESIDENT 3→

(DEMOCRATIC)
AL GORE PRESIDENT
JOE LIEBERMAN VICE PRESIDENT 5→

(LIBERTARIAN)
HARRY BROWNE PRESIDENT
ART OLIVIER VICE PRESIDENT 7→

(GREEN)
RALPH NADER PRESIDENT
WINONA LaDUKE VICE PRESIDENT 9→

(SOCIALIST WORKERS)
JAMES HARRIS PRESIDENT
MARGARET TROWE VICE PRESIDENT 11→

(NATURAL LAW)
JOHN HAGELIN PRESIDENT
NAT GOLDHABER VICE PRESIDENT 13→

A

OFFICIAL BALLOT, GENERAL ELECTION
PALM BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000

← 4 (REFORM)
PAT BUCHANAN PRESIDENT
EZOLA FOSTER VICE PRESIDENT

← 6 (SOCIALIST)
DAVID McREYNOLDS PRESIDENT
MARY CAL HOLLIS VICE PRESIDENT

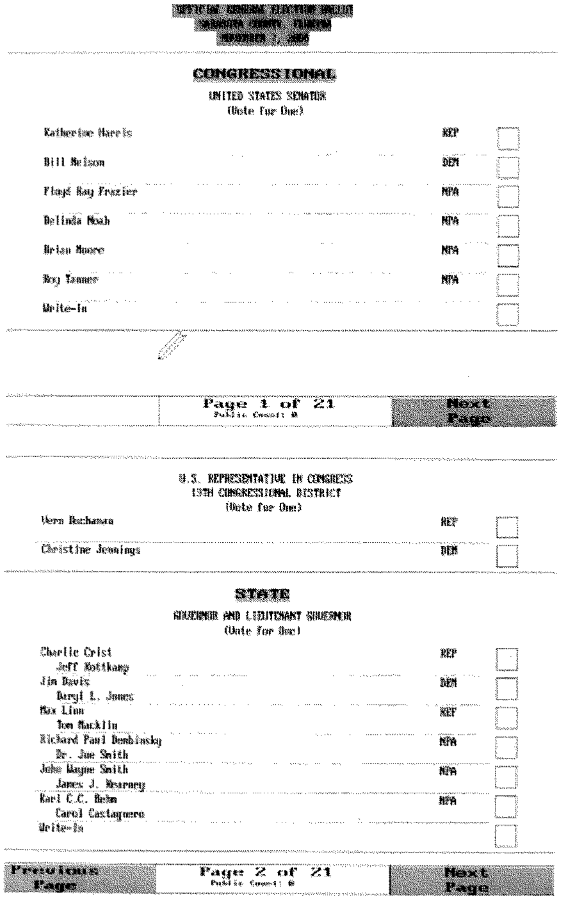
← 8 (CONSTITUTION)
HOWARD PHILLIPS PRESIDENT
J. CURTIS FRAZIER VICE PRESIDENT

← 10 (WORKERS WORLD)
MONICA MOOREHEAD PRESIDENT
GLORIA La RIVA VICE PRESIDENT

WRITE-IN CANDIDATE
To vote for a write-in candidate, follow the directions on the long stub of your ballot card.

FIGURE 4-1 Palm Beach County, Florida "Butterfly Ballot" from 2000 presidential election.
SOURCE: https://commons.wikimedia.org/wiki/File:Butterfly_Ballot,_Florida_2000_(large).jpg. Image is ineligible for copyright and therefore in the public domain because it consists entirely of information that is common property and contains no original authorship.

[71] See Wand, Jonathan N., et al., "The Butterfly Did It: The Aberrant Vote for Buchanan in Palm Beach County, Florida," *The American Political Science Review*, December 2001, Vol. 95, No. 4, pp. 793-810.



OFFICIAL GENERAL ELECTION BALLOT
SARASOTA COUNTY, FLORIDA
NOVEMBER 7, 2006

CONGRESSIONAL

UNITED STATES SENATOR
(Vote For One)

Katherine Harris	REP	□
Bill Nelson	DEM	□
Floyd Ray Frazier	NPA	□
Belinda Noah	NPA	□
Brian Moore	NPA	□
Roy Tanner	NPA	□
Write-In		□

U.S. REPRESENTATIVE IN CONGRESS
13TH CONGRESSIONAL DISTRICT
(Vote for One)

Vern Buchanan	REP	□
Christine Jennings	DEM	□

STATE

GOVERNOR AND LIEUTENANT GOVERNOR
(Vote for One)

Charlie Crist Jeff Kottkamp	REP	□
Jim Davis Daryl L. Jones	DEM	□
Max Linn Tom Macklin	REF	□
Richard Paul Dembinsky Dr. Joe Smith	NPA	□
John Wayne Smith James J. Kearney	NPA	□
Karl C.C. Behm Carol Castagnero	NPA	□
Write-In		□

FIGURE 4-2 Sarasota County, Florida electronic ballot from 2006 general election. The congressional race on page 2 may seem to be a continuation of the Senate race on the previous page, as it appears between two major statewide races, both of which are introduced by large, colored headings. The congressional race does not have such a heading.
SOURCE: Jefferson, David, "What Happened in Sarasota County?," *The Bridge*, 2007, Vol. 37, No. 2, pp. 21-22. Reprinted with permission from Jefferson (2007).

BOX 4-1
Ballot Design and the Disabled Community

Careful ballot design is especially important with respect to disabled voters. Paper ballots in particular can present special challenges for disabled voters. Most paper ballots do not provide full accessibility and verification capacity to voters with visual impairments. While there are technological solutions that can make paper more accessible (e.g., audio input for review and instructions), good, accessibility-focused electronic ballot design is as critical as good physical paper ballot design. A poorly designed audio ballot can be more confusing than a poorly designed printed ballot.

On Election Day, it can be difficult to train voters to cast a vote if procedures are not readily apparent. Votes are cast on machines that may be accessed only briefly every year or two and voters have only minutes to read and mark their ballots. Good ballot design principles are essential when electronic displays are used to present ballots on voting equipment and ballot-marking devices. Studies show that 43 percent of otherwise literate Americans (93 million people) encounter difficulty reading ballot instructions.[72] Greater than 60 percent of Americans older than age 65 have physical disabilities that make reading or hearing instructions difficult.[73]

The use of ballot-marking devices (BMDs) is increasing, as paper ballots present special challenges for disabled voters (see Box 4-1).

Findings

Poor ballot design can significantly affect the ability of voters to understand the choices presented as well as voters' ability to make selections that reflect their intent.

Poorly designed ballots continue to be used in elections. The embedding of specific ballot design criteria into statutes and regulations makes it difficult to counteract poor design principles.

Ballot design can help voters be successful if it follows proven com-

[72] Quesenbery, Whitney, Center for Civic Design, presentation to the committee, June 13, 2017, New York, NY, citing U.S. Department of Education, Institute of Education Sciences, National Center for Education Statistics, National Assessment of Adult Literacy, 2003.

[73] Golden, Diane Cordry, Association of Assistive Technology Act Programs, presentation to the committee, June 13, 2017, New York, NY.

munication and display design principles to meet voters' needs for easy interaction, plain language, consistency, and comprehension.

Good designs for electronically displayed ballots (e.g., designs that foster interaction, facilitate navigation, and incorporate plain language) are positive contributors to the voting experience.

RECOMMENDATION

4.9 State requirements for ballot design (inclusive of print, screen, audio, etc.) and testing should use best practices developed by the U.S. Election Assistance Commission and other organizations with expertise in voter usability design (such as the Center for Civic Design).

VOTING TECHNOLOGY

Meeting requirements for cost-effective and accessible voting requires attention to a variety of factors including: (1) accuracy and security; (2) the structure of the election technology market; (3) technology innovation; (4) certification and standards; and (5) the capacity and capability of election administrators to oversee technology acquisition and maintenance.

Many elections today are dependent on electronic voting and vote tabulation systems that collect, store, and process votes. Most voting systems make use of computers and computer networks, but current cybersecurity and auditing requirements have placed increased value on paper even in the context of computerized systems.

As discussed previously, following the 2000 election, through HAVA, Congress provided funding for states to improve election systems. HAVA gave particular attention to statewide voter registration systems and to the procurement of voting systems that would eliminate the problems associated with mechanical lever machines and punch cards in the 2000 presidential election.

Requirements for today's voting systems include: (1) support for contemporary voting modes and innovative processes such as early voting and vote by mail; (2) usability; (3) accessibility for disabled voters; (4) enhanced cybersecurity; and (5) auditability.

The post-2000 modernization of voting technologies sought to redress deficiencies associated with ballot designs, eliminate punch card systems in which recounts had been plagued by hanging chad, and complete the phase-out of long-obsolete mechanical voting machines.

Jurisdictions that replaced punch card or lever machines generally adopted either optical-scan or Direct Recording Electronic (DRE) voting machines.

DREs generally take the form of a custom computer with a screen to display the ballot. Voters indicate their selections using a touchscreen or a physical keypad. DREs typically employ specialized software running on top of commodity operating systems like Windows or Linux and a mix of standard and custom hardware. In most systems, tabulated votes are recorded in a removable memory module. Some DREs can transmit ballots or vote totals to a central location for the reporting of unofficial results. DREs may be used in precincts on Election Day or in vote centers or during early voting.

Early in their existence, DREs were attractive to some election administrators because they provided a modern, reliable upgrade from mechanical lever machines. DREs seemed convenient to use, because they provided instant tabulation at the close of the polls, and because they eliminated the need to preprint the correct number of paper ballots for all the voters in each precinct.

HAVA directed jurisdictions responsible for federal elections to provide at least one accessible voting system at each polling place. DREs were widely embraced as a solution to the challenge of making voting accessible to the disabled, even in many jurisdictions that adopted optical scan balloting for nondisabled voters.

Although DREs successfully addressed several concerns, they also introduced new challenges. Critics pointed out cybersecurity risks inherent in relying entirely on computers—thereby eliminating a voter-inspected paper artifact that could be manually counted.[74] DREs also introduced new usability problems associated with how ballots are displayed on a screen, how users navigate within and across screens, and how voter selections are made. They also introduced new technical challenges; touchscreen miscalibration, for example, can cause a voter's intended vote for one candidate to be misinterpreted as a vote for another candidate.

The purchase of DREs may require a high initial investment. DREs require software updates and the ongoing payments for technical support costs. Furthermore, DREs introduced new complexities to the vote casting process and are subject to technological obsolescence.

Voting machines that create voter-verifiable paper audit trails (VVPATs) have been introduced to address some of these concerns. A VVPAT is a printout that provides a physical record of a voter's selections. VVPATs are preserved as a physical record of a cast ballot. While VVPATs provide a physical record of a cast ballot, it is possible that the information stored in a computer's memory does not reflect what is printed on the VVPAT.

[74] See, e.g., Jones, Douglas W. and Barbara Simons, *Broken Ballots: Will Your Votes Count?* (Chicago: University of Chicago Press, 2012) and Verified Voting Foundation, "The Resolution on Electronic Voting," available at: https://www.verifiedvotingfoundation.org/projects/electronic-voting-resolution/.

Voters may inspect a VVPAT to see whether it reflects their intended selections before their votes are recorded in computer memory. If voters do not verify that the information on their VVPAT is accurate, inaccuracies may be recorded. Those with vision or other impairments or limitations may not, however, be able to perform this inspection. Furthermore, it may be difficult to track patterns of VVPAT errors that would indicate fraud. Finally, a combined approach that uses DREs and printers introduces complexity and adds new points of potential failure at the polling place.

Jurisdictions typically transmit ballots to those wishing to cast ballots via mail. Ballots may sometimes be retrieved from an elections website for printing and completion by remote voters. Some jurisdictions may also provide remote voters with software to prepare their ballots. While this software avoids problems associated with manual use of paper ballots such as undervotes and overvotes and spoiled ballots (as voters get immediate feedback before completing their ballots), it introduces additional security risks. Completed ballots are returned via mail, at designated collection points, or, in certain instances, by fax or via the Internet.

Well designed, voter-marked paper ballots are the standard for usability for voters without disabilities. Research on VVPATs has shown that they are not usable/reliable for verifying that the ballot of record accurately reflects the voter's intent, but there is limited research on the usability of BMDs for this purpose. BMDs moreover, may produce either a full ballot, a summary ballot, or a "selections-only" ballot. Unless a voter takes notes while voting, BMDs that print only selections with abbreviated names/descriptions of the contests are virtually unusable for verifying voter intent.[75]

Human beings must, however, interact not only with ballots, but also with all components of election systems. A usability failure of any particular component of an election system can be as detrimental as a failure of usability in the ballot. A voting system must be usable in a way that allows a voter to verify that the ballot of record correctly reflects his or her intent. Vote tabulation systems must be usable in a way that facilitates the correct tallying and tabulation of votes. Auditing technology must be useable in a way that enables efficient recounting.

Findings

Not all voting systems have the capacity for the independent auditing of the results of vote casting. Electronic voting systems that do not produce

[75] By hand marking a paper ballot, a voter is, in essence, attending to the marks made on his or her ballot. A BMD-produced ballot need not be reviewed at all by the voter. Furthermore, it may be difficult to review a long or complex BMD-produced ballot. This has prompted calls for hand-marked (as opposed to BMD-produced) paper ballots whenever possible.

a human-readable paper ballot of record raise security and verifiability concerns.

The software for casting and tabulating votes is not uniformly independent in voting systems.

Voting technology raises a particular set of issues for the disabled community.

Additional research on ballots produced by BMDs will be necessary to understand the effectiveness of such ballots.

RECOMMENDATIONS

4.10 States and local jurisdictions should have policies in place for routine replacement of election systems.

4.11 Elections should be conducted with human-readable paper ballots. These may be marked by hand or by machine (using a ballot-marking device); they may be counted by hand or by machine (using an optical scanner).[76] Recounts and audits should be conducted by human inspection of the human-readable portion of the paper ballots. Voting machines that do not provide the capacity for independent auditing (e.g., machines that do not produce a voter-verifiable paper audit trail) should be removed from service as soon as possible.

4.12 Every effort should be made to use human-readable paper ballots in the 2018 federal election. All local, state, and federal elections should be conducted using human-readable paper ballots by the 2020 presidential election.

4.13 Computers and software used to prepare ballots (i.e., ballot-marking devices) should be separate from computers and software used to count and tabulate ballots (scanners). Voters should have an opportunity to review and confirm their selections before depositing the ballot for tabulation.

VOTING SYSTEM CERTIFICATION

Overview and Analysis

Under HAVA, the EAC became responsible for developing and administering a voluntary system for federal certification of voting systems.[77] These

[76] A modern form of optical scanner, a *digital scanner,* captures, interprets, and stores a high-resolution image of the voter's ballot at a resolution of 300 dots per inch (DPI) or higher.

[77] U.S. Election Assistance Commission, "Testing & Certification Program Manual, Version 2.0," available at: https://www.eac.gov/assets/1/6/Cert_Manual_7_8_15_FINAL.pdf.

guidelines, known as the Voluntary Voting System Guidelines (VVSG), specify certain functional, accessibility, and security requirements for voting systems.

The EAC has two responsibilities pertinent to certification. First, with the technical assistance of the National Institute of Standards and Technology (NIST), the EAC oversees the development of the VVSG, which establishes the standards against which new voting systems are tested. Second, the EAC certifies independent voting system testing laboratories (VSTLs), which conduct the testing of new voting systems developed by commercial vendors.

States are ultimately responsible for determining the process by which voting systems will be certified in their states. Thirty-eight states and the District of Columbia rely on the federal testing and certification program, at least to some extent.[78] This can range from requiring that systems be tested to federal standards to requiring that systems be tested in federally approved laboratories. The remaining states do not require federal testing or certification per se, but in most cases rely on the federal certification program to guide their own state certification regimes. HAVA envisioned that the states might also perform testing of the accuracy, usability, and durability of the systems that they proposed to put into service.

The federal certification process begins only once a manufacturer has registered with the EAC Voting System Testing and Certification Program and has submitted a system for certification.[79] The process of certification can take up to 2 years. [80] Even then, a state certification process frequently follows after federal certification has been received. Following certification, other procedures, such as acceptance testing, logic and accuracy testing, and special purpose tests may follow. All told, the period between the develop-

[78] See National Conference of State Legislatures, "Voting System Standards, Testing, and Certification," available at: http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx.

[79] See "Testing & Certification Program Manual, Version 2.0." Systems are usually "submitted when (1) they are new to the marketplace, (2) they have never before received an EAC certification, (3) they are modified, or (4) the Manufacturer wishes to test a previously certified system to a different (newer) standard." See p. 19.

[80] Perez, Eddie, Hart InterCivic and Coutts, McDermot, Unisys Voting Solutions, presentations to the committee, December 8, 2017, Denver, CO. See also University of Pennsylvania, Wharton Public Policy Initiative, "The Business of Voting: Market Structure and Innovation in the Election Technology Industry," 2016, p. 38, available at: https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

ment of a new voting systems and its actual use in an election can last years and cost vendors millions of dollars.[81]

Current security standards certify equipment but not associated procedures and procedural requirements (e.g., auditing). This fact contributes to deficiencies in current standards.

Newly revised voluntary voting system guidelines, called VVSG 2.0, await final approval from the EAC. The new guidelines provide a more modular set of specifications and requirements against which voting systems can be tested to determine whether the systems provide basic functional, accessibility, and security capabilities required of these systems. This change is intended to foster the deployment of accurate and secure voting systems while also enabling system innovation that would allow the deployment of system upgrades in a timely fashion, facilitate interoperability of election systems, permit the transparent assessment of the performance of election systems, and provide a set of testable requirements that are easy to use and understand.[82] The approach of VVSG 2.0 focuses more on functional requirements than on the prescriptive specifics of the past. The draft guidelines require software independence for all voting systems in order to allow the correct outcome of an election to be determined even if the software does not perform as intended.[83,84]

Findings

Vendors and election administrators have expressed frustration with the certification process as presently implemented.

Costs and delays in the certification process may limit vendor innovation and increase system costs.

The requirements of the certification system can create barriers to

[81] The software used in voting systems is also subject to certification. This has important implications for system security. If the most recent version of particular software has not been certified, states may be forced to use an earlier software version with documented vulnerabilities.

[82] U.S. Election Assistance Commission, "VVSG Version 2.0: Scope and Structure," available at: https://www.eac.gov/assets/1/6/VVSGv_2_0_Scope-Structure(DRAFTv_8).pdf.

[83] "A voting system is software independent if an (undetected) change or error in its software cannot cause an undetectable change or error in an election outcome." See Rivest, Ronald L., "On the Notion of 'Software Independence' in Voting Systems," *Philosophical Transactions of the Royal Society A*, October 28, 2008, DOI: 10.1098/rsta.2008.0149. Dr. Rivest is a member of the committee that authored the current report.

An auditable voting system is software independent.

[84] The auditing of election results can reduce the need for certification and simultaneously provide better evidence that outcomes are correct. See, e.g., Stark, Philip B. and David A. Wagner, "Evidence-Based Elections," *IEEE Security and Privacy*, 2012, Vol. 10, DOI 10.1109/MSP.2012.62.

incremental improvements to systems that reflect improved manufacturing processes or software upgrades. This contributes to the process that has created a population of voting systems that have become obsolete (and therefore harder to secure) when compared even to the technology one encounters in today's typical office environment.

New approaches to the standards-setting and certification process (i.e., VVSG 2.0) have the potential to mitigate deficiencies in the current system.

RECOMMENDATIONS

4.14 If the principles and guidelines of the final Voluntary Voting System Guidelines are consistent with those proposed in September 2017, they should be adopted by the U.S. Election Assistance Commission.

4.15 Congress should:

a. authorize and fund the U.S. Election Assistance Commission to develop voluntary certification standards for voter registration databases, electronic pollbooks, chain-of-custody procedures, and auditing; and

b. provide the funding necessary to sustain the U.S. Election Assistance Commission's Voluntary Voting System Guidelines standard-setting process and certification program.

4.16 The U.S. Election Assistance Commission and the National Institute of Standards and Technology should continue the process of refining and improving the Voluntary Voting System Guidelines to reflect changes in how elections are administered, to respond to new challenges to election systems (e.g., cyberattacks), and to take advantage of opportunities as new technologies become available.

4.17 Strong cybersecurity standards should be incorporated into the standards-setting and certification processes at the federal and state levels.

5

Ensuring the Integrity of Elections

In this chapter, the committee discusses threats to the integrity of U.S. elections. Two topics that play critical roles in protecting this integrity, cybersecurity and auditing, are considered. The committee then assesses the widely proposed suggestion that ballots be cast via the Internet.

INTRODUCTION

There are numerous ways in which the integrity of elections can be affected. Election results may be improperly tallied or reported. Inaccuracies may be introduced by human error or because of a lack of proper oversight. Vote counts can be affected if fraudulent voting, e.g., multiple voting, illegal voting, etc., occurs. Election tallies and reporting may also be affected by malicious actors.

Malicious actors can affect vote counts by:

- introducing inaccuracies in the recording, maintenance, and tallying of votes; and/or
- altering or destroying evidence necessary to audit and verify the correct reporting of election results.[1]

There are many ways to prevent the casting of votes. Voters can be physically barred or otherwise deterred (e.g., by intimidation) from access-

[1] Other threats, e.g., disinformation campaigns, gerrymandering, etc., may affect election integrity and, while important, were viewed by the committee as outside of its charge.

ing polling sites. Information on voting locations, voting times, and voting processes may be manipulated to mislead potential voters. Disruptions in mail or Internet service may adversely affect remote voters. Registration data may be altered to disenfranchise voters. Voting equipment failures or inadequate supplies could prevent vote collection.

After votes have been cast, physical or electronic ballots can be altered, destroyed, or lost. Counting errors may affect manual or electronic tallying methods. Tallies may be inaccurately reported because of carelessness or malicious activity.

After the primary reporting of results, evidence that enables verification of the reported results may be altered or destroyed. This evidence could include original artifacts (e.g., cast ballots) or supplemental data provided to enable external auditing and verification.

Disruptions of Electronic Systems

Security vulnerabilities can be exploited to electronically disrupt voting or affect vote counts at polling locations or in instances of remote voting.

Denial-of-service Attacks

Denial-of-service (DoS) attacks interrupt or slow access to computer systems.[2] DoS can be used to disrupt vote casting, vote tallying, or election audits by preventing access to e-pollbooks, electronic voting systems, or electronic auditing systems.

When employed against even a limited number of jurisdictions, DoS disruptions could lead to a loss in confidence in overall election integrity. A DoS attack targeting select jurisdictions could alter the outcome of an election.

Malware

Malware—malicious software that includes worms, spyware, viruses, Trojan horses, and ransomware—is perhaps the greatest threat to electronic voting.[3] Malware can be introduced at any point in the electronic path of a

[2] If equipment is manipulated to slow its operation or compromise its operability, this may also constitute a DoS attack.

[3] Worms are standalone computer programs that replicate themselves in order to spread to other computers, possibly compromising the operability of the computers they infect now or in the future. Spyware is software that aims to gather information about a person or organization without their knowledge, that may send such information to another entity without the consumer's consent, or that asserts control over a device without the consumer's knowledge. A computer virus is a type of malicious software program that, when executed, replicates

vote—from the software behind the vote-casting interface to the software tabulating votes—to prevent a voter's vote from being recorded as intended.

Malware can prevent voting by compromising or disrupting e-pollbooks or by disabling vote-casting systems. It can prevent correct tallying by altering or destroying electronic records or by causing software to miscount electronic ballots or physical ballots (e.g., in instances where optical scanners are used in the vote tabulation process). Malware can also be used to disrupt auditing software.

Malware is not easily detected. It can be introduced into systems via software updates, removable media with ballot definition files, and through the exploitation of software errors in networked systems. It may also be introduced by direct physical access, e.g., by individuals operating inappropriately at points during the manufacturing of the election system or at the level of elections offices. It is difficult to comprehensively thwart the introduction of malware in all these instances.

Other Classes of Attacks

There are other avenues through which electronic systems may be disrupted. Malicious actors may obtain sensitive information such as usernames or passwords by pretending to be a trustworthy entity in an electronic communication. Servers may be breached to obtain administrator-level credentials. Individuals with site access (e.g., employees or contractors) might physically access a system.

Maintaining Voter Anonymity

If anonymity is compromised, voters may not express their true preferences. Anonymity can be compromised in many ways. Clandestine cameras at poll sites could be used to compromise voter anonymity. Latent fingerprints left on ballots might be used to link voters to their ballots. Full ballots dissociated from individual voters might be posted in the interest of ensuring transparency and/or to facilitate auditing, but it may be possible to tie particular ballots to individual voters. When voter anonymity is achieved using encryption, a failure in the encryption can lead to the disclosure of a voter's identity. With remote voting—voting outside of publicly monitored poll sites—it may not be difficult to compromise voter privacy. When voting, for example, by mail, fax, or via the Internet, individuals can

itself by modifying other computer programs and inserting its own code. Trojan horses are malicious computer programs that mislead users of their true intent. Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

be coerced or paid to vote for particular candidates outside the oversight of election administrators.

ELECTION CYBERSECURITY

Overview and Analysis

As described in Chapter 1, the Help America Vote Act (HAVA) prompted the acceleration of the introduction of electronic systems throughout the U.S. election process. There have since been concerns about vulnerabilities in the electronic systems that are used to perform most election functions. Given competing demands for attention and resources, these concerns have not always been a high priority for election administrators. However, citizen and government attention to these vulnerabilities greatly increased following reports of Russian efforts to compromise voter registration systems during the 2016 presidential election.

Attention brought to the problem of election cybersecurity during the 2016 election prompted energetic reactions from government, academia, and the public and private sectors. Following the U.S. Department of Homeland Security (DHS) designation of elections as critical national infrastructure, election administrators established the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) to improve information sharing among election officials. In addition, governmental and private-sector coordinating councils were established to share information and engage with DHS to address cyber threats to elections. In addition, organizations such as the Center for Internet Security and the Belfer Center at Harvard University have issued guides and "playbooks" to assist state and local officials in the mitigation of risks to their electronic system and in the adoption of best security practices.[4] Most recently, as part of the omnibus FY 2018 appropriations bill, the U.S. Congress appropriated $380 million "to the Election Assistance Commission for necessary expenses to make payments to States for activities to improve the administration of elections for Federal office, including to enhance election technology and make election security improvements."[5]

Election administrators face a daunting task in responding to cyber threats, as cybersecurity is a concern with all computer systems. This is

[4] See The Center for Internet Security, "A Handbook for Elections Infrastructure Security," available at: https://www.cisecurity.org/elections-resources/, and Belfer Center for Science and International Affairs, Harvard Kennedy School, "The State and Local Election Cybersecurity Playbook," available at: https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook.

[5] See H.R. 1625, Consolidated Appropriations Act, 2018, Section 501, available at: https://www.congress.gov/bill/115th-congress/house-bill/1625/text.

because (1) the design and development of current computer systems, no matter how well constructed, cannot anticipate and prevent all the possible means of attack; and (2) there are parties that will act in deliberately hostile ways to exploit vulnerabilities.

Vulnerabilities arise because of the complexity of modern information technology (IT) systems and human fallibility in making judgments about what actions are safe or unsafe from a cybersecurity perspective. Moreover, cybersecurity is a never-ending challenge. It is unlikely that permanent protections against cyber threats will be developed in the near future given that cybersecurity threats evolve and that adversaries continually adopt new techniques to compromise systems or overcome defenses. The general view is that the offense has the upper hand if the attacker is patient and well resourced. With respect to foreign threats, the challenge is compounded by the great asymmetry between the capabilities and resources available to local jurisdictions in the United States and those of foreign intelligence services.

Unfortunately, not all vendors or jurisdictions follow established best practices with respect to the development, maintenance, and operation of voting systems. This makes them more vulnerable to cyber-manipulation than they need to be. In comparison with other sectors (e.g., banking), many jurisdictions in the election sector are not following best security practices with regard to cybersecurity, one reason being that the banking industry is highly regulated, and part of these regulations is the supervision of their cybersecurity strategies.[6]

Several factors affect a bad actor's ability to compromise a system: (1) how well the system was designed; (2) whether the system is properly configured and updated; (3) how well the system is managed and operated; and (4) the skills, resources, and determination of the would-be attacker. Adoption of best practices for developing, testing, and management of systems can reduce (but not eliminate) the risk of a successful cyberattack. As a rule, stronger defenses increase the time and effort required to conduct an attack, and well-defended targets are less attractive to would-be attackers.

There are many layers between the application software that implements an electoral function and the transistors inside the computers that ultimately carry out computations. These layers include the election application itself (e.g., for voter registration or vote tabulation); the user interface; the application runtime system; the operating system (e.g., Linux or Windows); the system bootloader (e.g., BIOS or UEFI); the microprocessor firmware (e.g., Intel Management Engine); disk drive firmware; system-on-

[6] See, e.g., https://www.occ.treas.gov/news-issuances/news-releases/2017/nr-occ-2017-113.html and https://www.csbs.org/sites/default/files/2017-11/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf.

chip firmware; and the microprocessor's microcode. For this reason, it is difficult to know for certain whether a system has been compromised by malware. One might inspect the application-layer software and confirm that it is present on the system's hard drive, but any one of the layers listed above, if hacked, may substitute a fraudulent application layer (e.g., vote-counting software) at the time that the application is supposed to run. As a result, there is no technical mechanism that can ensure that every layer in the system is unaltered and thus no technical mechanism that can ensure that a computer application will produce accurate results. This has several important implications for election systems:

- all digital information—such as ballot definitions, voter choice records, vote tallies, or voter registration lists—is subject to malicious alteration;
- there is no technical mechanism currently available that can ensure that a computer application—such as one used to record or count votes—will produce accurate results;
- testing alone cannot ensure that systems have not been compromised; and
- any computer system used for elections—such as a voting machine or e-pollbook—can be rendered inoperable.

Election systems are especially vulnerable when they are connected to the Internet, telephone network,[7] or another wide-area network.[8] Systems that utilize network connections for their functions include voter registration systems, e-pollbooks, and post-election canvassing/reporting systems.

Even when systems are not directly connected to networks, they are vulnerable to attack through physical or wireless access.[9] They also are vulnerable whenever data transferred to them originates from another computer system that is itself vulnerable. For example, to attack a voting machine that receives data only through hand-carried removable media bearing "ballot definition files," an attacker might create a ballot definition file that takes advantage of a flaw in the software that reads a ballot definition file or displays a ballot.[10] Such an attacker need not be physically

[7] The telephone network is actually now part of the Internet. Land-line switching centers and cell-phone towers connect to each other through packet-switched networks (i.e., the technology underlying the Internet) that are connected to the larger Internet via border routers.

[8] Most wide-area networks are also connected to the larger Internet.

[9] Attacks are possible not only when systems are in use for elections but also during the manufacturing process or when such systems are in transit or in storage.

[10] Essentially every type of electronic voting machine must be programmed with ballot designs shortly before an election. As such, this is a particularly tempting attack vector, particularly for sophisticated actors.

present with that removable media—entry through a network-connected computer that creates the removable storage media may suffice (the removable storage media is used to transmit the ballot definition file).

Achieving stronger defenses against cyberattacks involves: (1) adopting state-of-the-art technologies and best practices more widely; and (2) developing new knowledge about cybersecurity. The first defense is primarily nontechnical and involves economic, organizational, and behavioral factors. The second defense requires research to develop new technologies and approaches.[11]

Cybersecurity and Vote Tabulation

Because there is no realistic mechanism to fully secure vote casting and tabulation computer systems from cyber threats, one must adopt methods that can assure the accuracy of the election outcome without relying on the hardware and software used to conduct the election. Uniform adoption of auditing best practices does not prevent tampering with the results collected and tabulated by computers. It can allow such tampering to be detected and often corrected. Good auditing practices can demonstrate that the results of an election accurately reflect the intention of the electorate without a need to trust the equipment used to conduct the election.

Cybersecurity and E-pollbooks

With respect to e-pollbooks and other election systems used during the election, independent backup systems are necessary in the event that primary systems become unavailable. E-pollbook data have traditionally been backed up with paper printouts. As an alternative, databases might be stored on static media such as DVDs. However, in jurisdictions that offer same-day registration or convenience voting in self-selected locations, relying on paper could lead to new risks of in-person voter fraud.[12] Addressing this risk by building fully independent systems (including independent networks connecting the polling sites) is not practical.[13]

[11] National Research Council, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues* (National Academies Press, Washington DC: 2014).

[12] While paper pollbooks will not proactively stop some forms of multiple voting, their use permits the retroactive detection of such activity and provides evidence against those acting illegally.

[13] In practice, there is no such thing as an independent network. See, e.g., footnote 7.

Factors that Exacerbate Cybersecurity Concerns

- *A highly decentralized elections system.* Because the U.S. elections system is highly decentralized, responsibility for cybersecurity often falls to the county or municipal level where expertise and resources may be quite limited.
- *Aging systems.* Because U.S. elections frequently make use of hardware and software that are aging—in some cases to the point that they would generally be considered obsolete—cybersecurity risk is increased because (1) such systems may fall well behind the current state of the art in cybersecurity measures; and (2) software or the operating system used to run it may no longer be receiving security updates.
- *Changing threat.* Traditionally, the goal has been to secure against election fraud by corrupt candidates or their supporters who may attempt to favor a particular candidate by altering or destroying votes or tampering with the vote tally. The 2016 election vividly illustrated that hostile state actors can also pose a threat. These actors often possess more sophisticated capabilities and can apply greater resources to the conduct of such operations. Moreover, they may have other goals than shifting the outcome for a particular candidate. If their goal is to disrupt an election or undermine confidence in its outcome, they may need only to achieve DoS against e-pollbooks or leave behind traces of interference like malicious software or evidence of tampering with voter registration lists or other records. Even failed attempts at interference could, if detected, cast doubt on the validity of election results absent robust mechanisms to detect and recover from such attacks.

Findings

There is no realistic mechanism to fully secure vote casting and tabulation computer systems from cyber threats.

U.S. elections are conducted using systems that are aging and prone to security vulnerabilities and operational failures. The continued use of outdated systems increases the possibility of a critical failure. Even if actual failures or compromises do not occur, there is a risk that public confidence in the electoral process could be undermined by the possibility of such compromise—especially if there are indications that such a compromise was attempted.

In comparison with other sectors (e.g., banking), the election sector is not following best security practices with regard to cybersecurity.

Data discrepancies are more difficult to detect in elections than in most other sectors because voters do not generally learn whether their votes were processed correctly.[14]

Even if best practices are applied, systems will not be completely secure.

Foreign state–sponsored attacks present a challenge for even the most responsible and well-resourced jurisdictions. Small, under-resourced jurisdictions are at serious risk.

Appropriate audits can be used to enable trust in the accuracy of election outcomes even if the integrity of software, hardware, personnel, or other aspects of the system on which an election is run were to be questioned.

Better cybersecurity is not a substitute for effective auditing.

RECOMMENDATIONS

5.1 **Election systems should continue to be considered as U.S. Department of Homeland Security–designated critical infrastructure.**

5.2 **The U.S. Election Assistance Commission and U.S. Department of Homeland Security should continue to develop and maintain a detailed set of cybersecurity best practices for state and local election officials. Election system vendors and state and local election officials should incorporate these best practices into their operations.**

5.3 **The U.S. Election Assistance Commission should closely monitor the expenditure of funds made available to the states for election security through the 2018 omnibus appropriations bill to ensure that the funds enhance security practices and do not simply replace local dollars with federal support for ongoing activities.[15] The U.S. Election Assistance Commission should closely monitor any future federal funding designated to enhance election security.**

5.4 **Congress should provide funding for state and local governments to improve their cybersecurity capabilities on an ongoing basis.**

ELECTION AUDITING

Overview and Analysis

Election audits are critical to ensuring the integrity of election outcomes and for raising voter confidence. Auditing can demonstrate the validity of

[14] End-to-end-verifiable systems have the capacity to demonstrate to voters that their votes were properly counted.

[15] See H.R. 1625, Consolidated Appropriations Act, 2018, Section 501, available at: https://www.congress.gov/bill/115th-congress/house-bill/1625/text.

an election outcome and provide an indication of errors in ballot tabulation. Effective auditing contributes to voting security by providing an answer to the question, "Can we trust the outcome of an election when the equipment (hardware and software) used to conduct the election may have vulnerabilities or when the process is subject to human error?"

For decades, traditional audits have been performed (and have been required by law) in many states. While election administrators have performed many types of post-election audits, such as process audits, the most widely known audits have been audits of cast ballots. Traditional ballot auditing requires that election results in some fixed percentage of precincts be reconfirmed by a hand count—though the details of actual implementation can reduce the value of the audit (election administrators should not, for example, always audit the same precincts).

Hand counting every ballot cast to be certain of the outcome is extremely time-consuming, and hand counts are susceptible to error or deliberate miscounting. The use of computerized voting machines provides flexibility and processing efficiencies. Nevertheless, computers are, as was discussed in the previous section, subject to programming errors, manipulation, and outside interference. Election audits have, therefore, become more important, as the performance of audits raises voter confidence in the reported outcomes of elections. The use of networked communication at various election stages has necessitated audits that address cybersecurity risks.

An evidence-based election would produce not only a reported (or initial) election outcome, but also evidence that the reported outcome is correct. This evidence may be examined in a "recount" or in a "post-election audit" to provide assurance that the reported outcome indeed is the result of a correct tabulation of cast ballots.

Voter-verifiable paper ballots provide a simple form of such evidence provided that many voters have verified their ballots. The ability of each voter to verify that a paper ballot correctly records his or her choices, before the ballot is cast, means that the collection of cast paper ballots forms a body of evidence that is not subject to manipulation by faulty hardware or software. These cast paper ballots may be recounted after the election or may be selectively examined by hand in a post-election audit. Such an evidence trail is generally preferred over electronic evidence like electronic cast-vote records or ballot images. Electronic evidence can be altered by compromised or faulty hardware or software.

Paper ballots are designed to provide a human-readable recording of a voter's choices. The term "paper ballot" here refers to a "voter-verifiable paper ballot," in the sense that voters have the opportunity to verify that their choices are correctly recorded before they cast their paper ballots. The voter may mark the ballot by hand, or the marked ballot may be produced by a voting machine. In the current context, the human-readable portion of the paper ballot is the official ballot of record that acts as the record of the voter's expressed choices.[16] Any human-readable, durable, tamper-evident medium such as cloth, cardstock, or plastic could be used instead of paper.

Statistical auditing techniques available now (and some in development) are more efficient and effective than earlier techniques wherein a predetermined percentage of precincts were recounted by hand to confirm the accuracy of initial precinct tallies. The implementation of statistical auditing techniques may require the allocation of additional time between the end of voting and when the official results of the election are certified.

Risk-Limiting Auditing

Auditing a fixed percentage of precincts may not provide adequate assurance with regard to the outcome of a close election. To address this weakness, a method of auditing known as risk-limiting auditing was developed.[17] Risk-limiting audits (RLAs) operate dynamically by examining individual randomly selected paper ballots until sufficient statistical assurance is obtained. This statistical assurance ensures that the chance that an incorrect reported outcome escapes detection and correction is less than a predetermined risk limit.

RLAs offer statistical efficiency. Auditing an election with tens of millions of ballots may require examining by hand as few as several hundred randomly selected paper ballots. A RLA might determine that more ballots need to be examined, or even that a full hand recount should be performed, if the contest is close or the reported outcome incorrect. Because RLAs layer a security mechanism (the risk-limiting audit itself) on top of the traditional vote-casting process, RLAs can often be performed without the adoption of new vote-casting processes. RLAs were piloted statewide in Colorado in 2017 and are now being piloted by several other states.[18]

[16] Rather than, for example, an electronic interpretation of the paper ballot or a non-human-readable barcode appearing on a ballot.

[17] For a general discussion of risk-limiting audits, see Lindeman, Mark and Philip B. Stark, "A Gentle Introduction to Risk-limiting Audits," *IEEE Security and Privacy*, Special Issue on Electronic Voting, 2012.

[18] The changes required to implement risk-limiting audits incur costs and require detailed planning, education, and development of required resources. Some states will, for example, need to adopt paper balloting (or purchase different scanners to be able to use comparison-based audits).

Executing an RLA for a single plurality contest in a single jurisdiction is not particularly challenging. Implementing an RLA for an election with multiple contests, multiple jurisdictions, multiple types of equipment, and multiple election types (not just plurality), requires more preparation, and a state (or other jurisdiction) should expect that the implementation process will take time.

The most efficient RLAs (comparison audits) make use of cast-vote records (CVRs) that electronically represent the contents of each paper ballot. A ballot-comparison audit operates by randomly selecting paper ballots from a list of all cast paper ballots on a ballot manifest and comparing the voter-verified human-readable contents of the selected paper ballots to the electronic records in the corresponding CVRs. When CVRs are not available (or cannot be linked to specific corresponding paper ballots), a ballot-polling audit may be used instead when margins are relatively large. Such an audit examines only randomly selected paper ballots (and no CVRs); however, many more paper ballots may need to be sampled and examined to achieve the same statistical assurance.[19]

RLAs can establish high confidence in the accuracy of election results—even if the equipment that produced the original tallies is faulty. This confidence depends on two conditions: (1) that election administrators follow appropriate procedures to maintain the chain-of-custody and secure physical ballots—from the time ballots are received, either in-person or by mail, until auditing is complete; and (2) that the personnel conducting the audit are following appropriate auditing procedures and the equipment and software used to audit the election are independent of the equipment and software used to produce the initial tallies. In the latter case, this not only requires that the software be independent of the software used to tally votes, but also that the software's specifications/algorithms, inputs, and outputs are transparent to permit members of the public to reproduce the software's operation.

End-to-end-verifiability

In recent years there has been increased interest in providing voters with an opportunity to verify that their votes have been accurately cast, counted, and tabulated. This presents a challenge due to the necessity of preserving the secrecy of the ballot. However, building upon cryptographic methods initially developed by computer scientist and cryptographer David Lee Chaum, researchers have developed an approach called end-to-end (E2E) verifiability. This approach enables voters and other members of the

In Colorado, the cost to the state to conduct its pilot of RLAs was $90,000 (Hall, Hilary, Boulder County (CO) Clerk and Recorder, presentation to committee, December 7, 2017, Denver, CO). Free & Fair, which developed the open-source tools used to conduct the Colorado RLA invested an additional $100,000 in the effort (Kiniry, Joe, Free & Fair, presentation to committee, December 7, 2017, Denver, CO).

[19] Not all optical scanners can produce CVRs that can be linked to specific paper ballots; linked CVR–based RLAs are more efficent and cost-effective than ballot-polling RLAs; therefore, the ability to produce linked CVRs is an important consideration when purchasing and deploying voting machines.

public to audit the integrity of an election without relying on hardware, software, or personnel associated with elections.[20]

An election is E2E-verifiable (E2E-V) if it achieves three goals: 1) voters can obtain assurance that their selections have been properly recorded; 2) any individual can verify that his or her ballots have been included in vote tallies; and 3) members of the public can verify that the final tally is the correct result for the set of ballots collected. E2E-verifiability enables not only detection of external threats, but also detection of internal threats including errors or tampering by election officials, corrupted equipment, or compromises originating with equipment vendors.

E2E-V voting systems adopt certain properties (see Box 5-1), encrypt ballot data, and permit verification of data throughout the voting process. In an election context, "end-to-end" refers to the flow of ballot data through the entirety of the voting process and to the idea that the data may be verified at multiple stages in the voting process. The phrase should not, however, be interpreted to mean that verification must occur at particular stages of the process.

E2E-verifiability is a property that may be achieved in an election—rather than a particular methodology. Systems with various characteristics have been designed to produce E2E-V elections. In practice, an E2E-V voting system might work as follows:

> Upon marking a ballot, the voter would obtain a receipt which is a "cryptographically-masked" copy of the voter's selections (the voter's choices would thus not be visible in a way that would enable vote-selling or coercion). The receipt could be machine-issued or derived from the process of marking a pre-printed paper ballot.
>
> There are several methods to test whether the encryption process is working properly. In one scenario, voters might be allowed to "spoil" one or more ballots after receipts have been produced.[21] Voters could subsequently verify that receipts issued for spoiled ballots accurately reflect selections made. Because voting systems cannot predict whether a voter

[20] For a general discussion of end-to-end (E2E) election verifiability, see Benaloh, Josh, et. al, "End-to-end Verifiability," 2014, available at: https://pdfs.semanticscholar.org/4650/db843e0e90ca7ff54c7fe8e6080d12f6a0fc.pdf. Dr. Benaloh is a member of the committee that authored the current report. Dr. Ronald L. Rivest, who is also a member of the committee that authored the current report, was a co-author of the paper and has authored other papers on end-to-end verifiability.

[21] A *spoiled ballot* is a ballot that is invalidated and not included in the vote tally. Ballots might be spoiled accidentally or deliberately. A ballot may be spoiled in many ways (e.g., if the ballot is defaced, if invalidating stray marks are added to the ballot, etc.).

Voters would be permitted to verify the accuracy of the encryption only on spoiled ballots. This is to ensure that the verification process could not be used to reveal how individuals actually voted.

BOX 5-1
Properties of End-to-end-verifiable Voting Systems

End-to-end-verifiable (E2E-V) voting systems share the following security properties:

Integrity. Once a voter successfully enters his or her ballot into an E2E-V system, it cannot be undetectably lost or modified in any way, even in the presence of computer bugs or malicious logic.

Counting Accuracy. Ballots cannot be miscounted without the miscount being detectable.

Public Verifiability. E2E-V systems provide outputs and publish sufficient verification data to permit any voter to verify that his or her ballot was not lost or modified and that votes were properly tabulated. Verification data provides cryptographic proof that ballot integrity was preserved and tabulation was correct. Anyone may run a verification program on the verification data to confirm the accuracy of the data.

Transparency. Mathematical principles underlying the E2E-V security guarantees are open and public. The specifications for verification programs are publicly documented, and voters and observers are free to create and execute their own verification programs.

SOURCE: Adapted from U.S. Vote Foundation, "The Future of Voting: End-to-end Verifiable Internet Voting," July 2015, p. 111, available at: https://www.usvotefoundation.org/sites/default/files/E2EVIV_full_report.pdf.
Dr. Ronald L. Rivest and Dr. Josh Benaloh, members of the committee that authored the current report, made contributions to the U.S. Vote Foundation report.

will spoil a ballot, a voting system must correctly encrypt all receipts, as only a small fraction of voters would need to verify that spoiled ballots have been properly encrypted to reveal systematic erroneous behavior by a voting system.

After polls close, copies of all voter receipts would be posted to a public electronic bulletin board in order to allow voters to confirm that their votes have been properly recorded. If the voter's unique receipt was not posted, the voter could file a protest and use the receipt as evidence for correcting the posting error.

All voter receipts would be processed using a series of cryptographic computations that would yield the results of the particular election. The algorithms and parameters for the cryptographic operations would be posted on a website to enable voters to verify that their votes were tallied as recorded and to allow other observers to verify that the tally is correct.[22]

When E2E-verifiability is used with paper ballots, conventional recounts and risk-limiting audits are possible as additional means of verification.

E2E-verifiablility adds complexity to the election process, and the effective wide-scale deployment of E2E-verifiability will require a broad understanding of the underlying cryptographic methods by election officials and the general public. It may initially be challenging to understand the tools that could be employed to make E2E-verifiability possible.[23] Further, with E2E-V systems, it is possible that the encryption of voter receipts could be compromised. While such decryption would not affect the integrity of an election, it could compromise voter anonymity.

E2E-V methods seem to be necessary for secure voting via the Internet, but the methods are, in and of themselves, insufficient to address all of the security issues associated with Internet voting. Electronic versions of ballots may be subject to Internet-based (or other) attacks that might, for example, delete electronic ballots or otherwise replace or modify electronic election records. With E2E-V systems—as with any voting system—a bad actor could simply claim that his or her vote was not accurately captured. Such claims could eventually be discounted by security experts following the E2E-V trail of evidence. However, with sufficient numbers of bad actors acting simultaneously, confidence in an election outcome could be eroded before all the necessary independent verifications could take place.[24]

[22] Ali, Syed Taha and Murray, Judy, "An Overview of End to End Verifiable Voting Systems," in *Real-World Electronic Voting: Design, Analysis and Deployment*, Hao, Feng and Peter Y.A. Ryan, eds. (Boca Raton: CRC Press, 2016).

[23] For one fielded E2E-verification system (Scantegrity) used twice in elections in Takoma Park, MD, the voting process was seen as so much like that experienced previously with optical scan systems that voters did not notice the additional E2E-verifiability mechanisms. With other systems, it is possible that the impact of adding E2E-verification features would be more noticeable.

Scantegrity is paper-based insofar as the casting of ballots. It only uses the Internet as a means through which voters may verify that their votes were included in the tally, or by which anyone can verify that a vote tally is correct, given the posted votes.

[24] Some E2E-verifiable (E2E-V) systems provide mechanisms to address this threat. With the Scantegrity system, for example, voters mark their paper ballots with special pens that reveal a secret code when a voter selects a candidate (the code changes with each ballot). A voter cannot credibly claim to have voted for a candidate without knowing the associated code.

Findings

Complicated and technology-dependent voting systems increase the risk of (and opportunity for) malicious manipulation. Additional methods of review help reduce risks and detect violations of desired security properties.

Conducting rigorous audits enhances confidence in the correctness of election outcomes.

Risk-limiting audits can efficiently establish high confidence in the correctness of election outcomes—even if the equipment used to cast, collect, and tabulate ballots to produce the initial reported outcome is faulty.

States and jurisdictions purchasing election systems should consider in their purchases whether the system has the capacity to match CVRs to physical ballots, as this feature could result in future cost savings when audits are conducted.

While achieving E2E-verfiability, one must still preserve the secret ballot. E2E-V systems generally achieve this by using cryptographic methods to "mask" ballot data while preserving the ability for voters and observers to verify that ballots have been tallied correctly.

E2E-verifiability protocols are not, in and of themselves, sufficient to secure Internet voting, even in theory.

E2E-V election systems enable members of the public to conduct their own audits (or have audits conducted by independent, trusted third parties of their choice).

E2E-V elections can utilize paper ballots or operate purely electronically, the latter offering a means of auditing elections that support voters with visual and/or motor-skill limitations.

Risk-limiting auditing and public auditing using E2E-verifiability may address some security risks associated with tampering. The techniques can be used in combination.

RECOMMENDATIONS

5.5 **Each state should require a comprehensive system of post-election audits of processes and outcomes. These audits should be conducted by election officials in a transparent manner, with as much observation by the public as is feasible, up to limits imposed to ensure voter privacy.**

5.6 **Jurisdictions should conduct audits of voting technology and processes (for voter registration, ballot preparation, voting, election reporting, etc.) after each election. Privacy-protected audit data should be made publicly available to permit others to replicate audit results.**

5.7 Audits of election outcomes should include manual examination of statistically appropriate samples of paper ballots cast.

5.8 States should mandate risk-limiting audits prior to the certification of election results. With current technology, this requires the use of paper ballots.[25] States and local jurisdictions should implement risk-limiting audits within a decade. They should begin with pilot programs and work toward full implementation. Risk-limiting audits should be conducted for all federal and state election contests, and for local contests where feasible.

5.9 State and local jurisdictions purchasing election systems should ensure that the systems will support cost-effective risk-limiting audits.

5.10 State and local jurisdictions should conduct and assess pilots of end-to-end-verifiable election systems in elections using paper ballots.

INTERNET VOTING

Overview and Analysis

As more aspects of people's lives move online, it is natural to ask whether the future of voting will also be online. Many people are familiar with and comfortable with the Internet as a tool and conduct what might be considered high-risk transactions (e.g., banking, e-commerce, the transmission of medical records, etc.) online. Internet voting has the potential to increase convenience and perhaps increase participation.[26] With Internet voting, all ballots would be marked using software run on a special voting station or on a voter's own smartphone, tablet, laptop, or desktop computer. Completed ballots would then be transmitted electronically to be tabulated. Although Internet voting offers convenience, it introduces new risks with regard to the integrity and confidentiality of votes as well as the potential for cyberattacks that could make it difficult or impossible for voters to cast their ballots within

[25] Risk-limiting audits examine individual randomly selected paper ballots until there is sufficient statistical assurance to demonstrate that the chance that an incorrect reported outcome escaping detection and correction is less than a predetermined risk limit.

[26] Katherine Stewart and Jirka Taylor, analysts for the RAND Corporation, recently concluded that "the observed impact of online voting on voting behaviour to date has been varied. In some cases, it has led to an initial increase in voter turnout. But whether this leads to a long-term trend of sustained voter engagement, particularly among younger people, remains unclear." Citing numerous sources, Stewart and Taylor suggest that online voting "may not be the 'silver bullet' in addressing the wider problem of voter disengagement." See https://www.rand.org/blog/2018/03/online-voting-the-solution-to-declining-political-engagement.html?adbid=986626411103379461&adbpl=tw&adbpr=22545453&adbsc=social_20180418_2261001.

the voting period. Furthermore, the casting of a ballot is an anonymous one-time event. This scenario makes it difficult to identify and correct a miscast vote.

Insecure Internet voting is possible now, but the risks currently associated with Internet voting are more significant than the benefits. Secure Internet voting will likely not be feasible in the near future.

Many vendors, however, currently offer Internet voting systems. Private elections (e.g., corporate shareholder elections) are often conducted primarily over the Internet. Some public elections have allowed Internet voting as an option or even used the Internet as the sole medium for casting votes. As discussed on page 68, voting by fax is sometimes allowed for absentee voters, and completed ballots are sometimes accepted as email attachments.

To ensure secure Internet voting, voters must be supplied with suitable digital credentials that allow them to prove their identity when voting online. Such credentials are supplied to all citizens in some nations (e.g., Estonia). These credentials allow individuals to access a variety of government services. Estonia has extended these services to voting.[27] Neither the U.S. federal government nor the states seem likely to supply universal digital credentials in the near future.[28] If voting is the only purpose for which these credentials are used, voters might easily surrender their credentials to others. Simple PINs and passwords are inadequate for secure voting, and standard email is an inappropriate medium for distributing strong credentials or transmitting marked ballots.[29]

[27] Digital credentials may be vulnerable to hacking. In 2017, Estonia suspended the use of its identity smartcards in response to the discovery of a wide-ranging security flaw. More than 750,000 ID cards were affected. See, e.g., "Estonia Has Frozen Its Popular E-Residency ID Cards Because of a Massive Security Flaw," *Business Insider*, November 6, 2017, available at: http://www.businessinsider.com/estonia-freeze-e-residency-id-cards-id-theft-2017-11.

[28] The federal government does provide Common Access Cards (CACs). CACs are "'smart card[s]' about the size of a credit card." They are "standard identification for active duty uniformed Service personnel, Selected Reserve, DoD [U.S. Department of Defense] civilian employees, and eligible contractor personnel . . . [and] the principal card used to enable physical access to buildings and controlled spaces, and" provide "access to DoD computer network and systems." See http://www.cac.mil/common-access-card/.

[29] See, e.g., U.S. Vote Foundation, "The Future of Voting: End-to-end Verifiable Internet Voting—Specifications and Feasibility Study," July 2015, p. 112, available at: https://www.usvotefoundation.org/sites/default/files/E2EVIV_full_report.pdf.

Obstacles to Internet Voting

Many concerns must be addressed before secure Internet voting would be feasible.[30]

Malware

The malware threat present whenever software is used is amplified in the case of Internet voting when voters use personal devices. Such devices may be less well tended and protected than the dedicated election equipment maintained by election officials.

Denial-of-service Attacks

While denial-of-service (DoS) is a risk in any voting medium, it is a mainstay of today's Internet. Many vendors provide services that can mitigate, but not eliminate, these attacks. Unfortunately, the mitigations usually require full decryption of all transmitted data, and these services are performed on systems that are shared with numerous third parties.

Related Technologies

Several technologies are directly relevant to Internet voting.

Secure Channel Technologies

Email is an Internet technology. Most email does not utilize the secure channel technologies commonly used for applications such as online banking and shopping. This makes email voting more vulnerable than many other forms of Internet voting.

Most fax transmissions travel, at least in part, over the Internet and therefore should also be regarded as a form of Internet voting with all of the added risks.

Blockchains

Blockchains are a technology meant to achieve an unalterable, decentralized, public, append-only log of transactions, without any single authority in a position to change the log. In an election context, the "transactions" would be the casting of ballots. A blockchain could therefore act as a virtual electronic ballot box. Blockchains may be managed publicly or by a

[30] In addition to the concerns described below, server-side break-ins (demonstrated against the Washington, DC, system in 2010), man-in-the-middle attacks (demonstrated against New South Wales in 2015), and authentication technology vulnerabilities (discovered in Estonia's system in 2017) represent other obstacles that must be addressed before Internet voting would be feasible.

restricted set of managers.[31] Several companies provide, or are attempting to build, voting systems around blockchains.[32]

While the notion of using a blockchain as an immutable ballot box may seem promising, blockchain technology does little to solve the fundamental security issues of elections, and indeed, blockchains introduce additional security vulnerabilities. In particular, if malware on a voter's device alters a vote before it ever reaches a blockchain, the immutability of the blockchain fails to provide the desired integrity, and the voter may never know of the alteration.

Blockchains are decentralized, but elections are inherently centralized. Although blockchains can be effective for decentralized applications, public elections are inherently centralized—requiring election administrators define the contents of ballots, identify the list of eligible voters, and establish the duration of voting. They are responsible for resolving balloting issues, managing vote tabulation, and announcing results. Secure voting requires that these operations be performed verifiably, not that they be performed in a decentralized manner.

While it is true that blockchains offer observability and immutability, in a centralized election scenario, observability and immutability may be achieved more simply by other means. Election officials need only, for example, post digitally signed versions of relevant election-related reports for public observation and download.

Ballots stored on a blockchain are electronic. While paper ballots are directly verifiable by voters, electronic ballots (i.e., ballots on a blockchain) can be more difficult to verify. Software is required to examine postings on blockchain. If such software is corrupted, then verifiability may be illusory. Software independence is not, therefore, achieved through posting ballots on a blockchain: as ballots are represented electronically, software independence may be more difficult to achieve.

The blockchain abstraction, once implemented, provides added points of attack for malicious actors. For example, blockchain "miners" or "stakeholders" (those who add items to the blockchain) have discretionary control over what items are added. Miners/stakeholders might collude to suppress votes from certain populations or regions. Furthermore, blockchain protocols generally yield results that are a consensus of the miners/stakeholders. This consensus may not represent the consensus of the voting public. Miners/stakeholders with sufficient power might also cause confusion and uncertainty about the state of a blockchain by raising doubts about whether a consensus has been reached.

[31] Blockchains managed by a restricted set of managers are referred to as *provisioned blockchains*.

[32] Voatz, Inc. and Votem are two such companies.

Blockchains do not provide the anonymity often ascribed to them.[33] In the particular context of elections, voters need to be authorized as eligible to vote and as not having cast more than one ballot in the particular election. Blockchains do not offer means for providing the necessary authorization.

Blockchains do not provide ballot secrecy. If a blockchain is used, then cast ballots must be encrypted or otherwise anonymized to prevent coercion andvote-selling. While E2E-V voting methods may provide the necessary cryptographic tools for this, ordinary blockchain methods do not.

It may be possible to employ blockchains within an election system by addressing the security issues associated with blockchains through the use of additional mechanisms (such as, for example, those provided by E2E-verifiability), but the credit for addressing such problems would lie with the additional mechanisms, not with the use of blockchains.

End-to-end-verifiable Systems

End-to-end-verifiable (E2E-V) technologies can be used in a variety of voting scenarios.

In its 2015 report, the U.S. Vote Foundation asserted that any possible future Internet voting system should utilize E2E-verification, but the report stated that this should not even be attempted before greater experience has been garnered with E2E-V systems deployed and used within in-person voting scenarios.[34]

E2E-V voting mitigates some of the vulnerabilities in Internet voting. However, advances in prevention of malware and DoS attacks need to be realized before *any* Internet voting should be undertaken in public elections—even if E2E-V.

[33] A July 13, 2018 federal indictment of twelve Russian operatives, for instance, describes in detail how the operatives were traced and identified through their use of the cryptocurrency bitcoin and its associated blockchain ledger. Count Ten of the indictment (Conspiracy to Launder Money) details how "the Conspirators" used bitcoin and its blockchain ledger in an attempt to "obscure their identities and their links to Russia and the Russian government" and how their use of bitcoin, despite the "perceived anonymity" of blockchains, was then exploited by investigators to identify the operatives. See *United States of America vs. Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukashev, Sergey Aleksandrovich Morgachev, Nikolay Yuryevich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevich Malyshev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, and Anatoliy Sergeyevich Kovalev*, Case 1:18-cr-00215-ABJ (2018), pp. 21-22, available at: https://www.justice.gov/file/1080281.

[34] "The Future of Voting: End-to-end Verifiable Internet Voting—Specifications and Feasibility Study," p. v.

Findings

All Internet voting schemes (including those that are E2E-V) are vulnerable to DoS attacks.

The Internet is not currently a suitable medium for the transmission of marked ballots, as Internet-based voting systems in which votes are cast on remote computers or other electronic devices and submitted electronically cannot be made adequately secure today.

E2E-verifiability may mitigate many of the threats associated with Internet voting.

Conducting secure and credible Internet elections will require substantial scientific advances.

The use of blockchains in an election scenario would do little to address the major security requirements of voting, such as voter verifiability. The security contributions offered by blockchains are better obtained by other means. In the particular case of Internet voting, blockchain methods do not redress the security issues associated with Internet voting.

RECOMMENDATIONS

5.11 At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots.[35,36] Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.[37]

5.12 U.S. Election Assistance Commission standards and state laws should be revised to support pilot programs to explore and validate new election technologies and practices. Election officials are encouraged to seek expert and public comment on proposed new election technology before it is piloted.

[35] Inclusive of transmission via email or fax or via phone lines.

[36] The Internet is an acceptable medium for the transmission of unmarked ballots to voters so long as voter privacy is maintained and the integrity of the received ballot is protected.

[37] If secure Internet voting becomes feasible and is adopted, alternative ballot-casting options should be made available to those individuals who do not have sufficient access to the Internet.

6

Analysis of Systemic Issues

In this chapter, the committee discusses election administrator and poll worker training, the voting technology marketplace, and the federal role in elections.

ELECTION ADMINISTRATOR AND POLL WORKER TRAINING

Overview and Analysis

Proper training of election administrators is a key component in ensuring well-run elections and in the mitigation of disruptions in the voting process.

Voting jurisdictions in the United States come in many sizes. Fully one-third are small towns with small budgets, part-time and volunteer staff, and limited access to information technology (IT) expertise. Between and during elections, staff generally have other responsibilities (e.g., recording deeds, issuing licenses, etc.). In most locations, poll workers have minimal training. They work intermittently during election cycles, often only on Election Day.

In larger jurisdictions, election administrators supervise larger staffs who may have attended some continuing education classes on election management offered by other in-state organizations of local public officials or the state election authority. In-service groups such as The Election Center,[1] along with national organizations of public officials, offer profes-

[1] See https://www.electioncenter.org/.

sional certificate programs in election administration. Auburn University, the University of Minnesota, and Kennesaw State University (Georgia) offer undergraduate and graduate courses in election management.[2] Courses include an introduction to the election process, election design, data analysis, voter participation, and strategic management. Courses in cybersecurity are beginning to be offered. Although some jurisdictions (e.g., Los Angeles County and New York State) now require training certification for election workers, there are no national accrediting standards for an election management curriculum at universities or community colleges.

Modern elections are more complex and consequently require election administrators with more specialized skills. Training and education programs in election administration are limited, and there are scant resources available to professionalize the election workforce. Many election administrators receive only minimal professional education and training beyond on-the-job experience. Increasing technical and management challenges require staff with more advanced qualifications and training, and it may be necessary to bring skilled people from other disciplines (including but not limited to IT and cybersecurity) into election administration. This reality may necessitate a review of hiring practices by election administrators.

Because most election administrators have other responsibilities, time and access to education and training opportunities are limited. Tight municipal and county budgets compound these constraints. Cross-institutional cooperation may provide a means of lowering barriers to better training and education in those communities with limited resources.

State and local election administrators are highly dependent on system vendors to install and maintain election systems, and they do not have access to the most comprehensive and current resources for implementing, checking, and making enhancements to the IT supporting their election systems.

Findings

There is a need to develop the professional election workforce in ways that enable it to handle new challenges in election administration.

There are growing gaps in election administrators' information technology skills, in their ability to access skilled IT professionals, and in their ability to detect, prevent, and respond to cyberattacks.

[2] Hale, Katherine, Auburn University, presentation to the committee, December 8, 2017, Denver, CO.
Further, the Network of Schools of Public Policy, Affairs, and Administration (NASPAA) is establishing an "Election Commons" through which schools can collaborate on course development and cross-registration in election administration offerings. See http://www.naspaa.org/students/InternshipSum17_ElectionAdministration.pdf.

RECOMMENDATIONS

6.1 Congress should provide adequate funding for the U.S. Election Assistance Commission to continue to serve as a national clearinghouse of information on election administration.

6.2 The U.S. Election Assistance Commission, with assistance from the national associations of state and local election administrators, should encourage, develop, and enhance information technology training programs to educate state and local technical staff on effective election administration.

6.3 Universities and community colleges should increase efforts to design curricula that address the growing organizational management and information technology needs of the election community.

THE VOTING TECHNOLOGY MARKETPLACE

Overview and Analysis

The 2000 presidential election was the impetus for a national transition from mechanical to electronic voting machines and from manual to automated processes. The election thrust the shortcomings of punch card voting technology into the spotlight and exposed a need for more reliable voting systems. As part of the 2002 Help America Vote Act (HAVA), Congress authorized the allocation of $3 billion to the states, primarily for the purchasing of new voting technology.[3] HAVA also created the U.S. Election Assistance Commission (EAC), an independent entity that would "serve as a national clearinghouse and resource for the compilation of information and review of procedures with respect to the administration of Federal elections"[4] and develop "voluntary voting system guidelines."[5] The EAC was responsible for administering HAVA funds.

The infusion of HAVA funding led to the development and deployment of new voting machines, and in particular, a more widespread deployment of Direct Recording Electronic (DRE) devices.The EAC reports that, "through September 30, 2015, a total of $3,247,294,645 has been made

[3] See HAVA Section 101. In addition to upgrading voting systems, states were to use HAVA funds for the purposes of "improving the administration of elections for Federal office;" "educating voters concerning voting procedures, voting rights, and voting technology;" "training election officials, poll workers, and election volunteers;" and "improving the accessibility and quantity of polling places, including providing physical access for individuals with disabilities, providing nonvisual access for individuals with visual impairments, and providing assistance to Native Americans, Alaska Native citizens, and to individuals with limited proficiency in the English language."

[4] See HAVA, Part 1, Election Assistance Commission.

[5] See HAVA Part 3, Section 221.

available to the 50 States, American Samoa, the District of Columbia, Guam, the Commonwealth of Puerto Rico and the United States Virgin Islands (hereinafter referred to as States) under HAVA" and that "States have reported total expenditures of $3,197,438,400 or 89 percent of total Federal funds and accrued interest available" to them.[6] Looked at another way, "36 of 55 (65 percent) states and territories in the US have less than 10 percent of their originally allocated HAVA funds left (including interest) and another 14 states and territories (25 percent) have less than half of their funding left."[7]

HAVA provided much-needed funding for improved voting technology. However, at the time the Act was passed, available machines had flaws related to both security and operational aspects. For instance, DRE machines did not produce a means for voter verification and did not adequately address the needs of the disabled community. Furthermore, HAVA provided only a one-time infusion of funds. There were no provisions to provide funding for the replacement of voting machines in the future, and to satisfy statutory requirements, many states made significant equipment purchases at the onset of funding. The conduct of elections is, however, an ongoing (and evolving process) and periodic infusions of funding do not allow for a consistent program of improvements.

"The depletion of the HAVA funds has significant implications today, as the systems deployed as a result of HAVA are nearing the end of their useful life and need to be replaced. The service life of most new voting hardware and software purchased and installed immediately after the passing of HAVA is 10-15 years, and states now lacking HAVA funds have to go to extraordinary lengths to keep their aging systems operational."[8]

"The election technology industry has come to be characterized by a consolidated, highly concentrated market dominated by a few major vendors, where industry growth and competition are constrained." "The firms in the election technology industry sell integrated voting solutions, typically including a package of hardware, software, services and support. The industry has a two-tier structure with . . . Election Systems and Software ("ES&S"), Hart Intercivic ("Hart") and Dominion Voting Systems," the largest vendors, in the top tier.[9] In the second tier, a few small firms provide

[6] U.S. Election Assistance Commission, "Annual Grant Expenditure Report, Fiscal Year 2015," p. 2, available at: https://www.eac.gov/assets/1/28/Final%20FY%202015%20Grants%20Report.pdf.

[7] See University of Pennsylvania, Wharton School Public Policy Initiative, "The Business of Voting: Market Structure and Innovation in the Election Technology Industry," 2016, p. 12, available at: https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

[8] Ibid, p. 13.

[9] Ibid, pp. 14-15. From this tier, the committee received testimony from Hart InterCivic. ES&S and Dominion Voting Systems declined to make presentations to the committee.

specialized technology (e.g., for the disabled) or serve small markets.[10] The largest voting technology vendor, ES&S, has about 460 employees. The customer base for voting machines is fragmented, and purchasers have widely varying levels of technological and purchasing expertise. Furthermore, buying power is limited for all but the largest customers.

The price of voting machines is usually not made public, and costs vary depending on factors such as the number of units purchased, the vendor chosen, and whether or not maintenance agreements are also purchased. The National Conference of State Legislatures (NCLS) estimates that the cost of a DRE voting machine ranges from $2,500 to $3,000 per unit, exclusive of peripherals such as voter-verified paper audit trail (VVPAT) and accessibility features. NCLS estimates that the cost per unit for precinct optical scanners ranges from $2,500 to $5,000 and that the cost of a central count optical scanner ranges from $70,000 to $100,000.[11] "The Brennan Center estimates it could cost well over $1 billion to replace all of the voting machines that should be replaced in the next few years."[12]

Some election administrators are exploring alternatives to the current private-sector, for-profit marketplace for election systems. Several jurisdictions are exploring the development of open-source or publicly-owned voting systems that use commercial off-the shelf (COTS) hardware in an effort to reduce both the initial cost and ongoing software maintenance costs associated with proprietary systems.

The usual model of open-source software is that with a license, a user has access to the source code and can read, use, or modify it in accordance with the license.[13] Widely used open source software is normally maintained by an organization that provides documentation and distribution sites. Any software developer can propose software changes and modifications, which are vetted by one or more experts, who integrate the changes into the distributed software. Hence the organization creates a kind of standardization, for users whose individual modifications are limited. The transparency provided by the availability of source code increases confidence that the software functions as intended. The participation of the user community aids software quality (since problems are publicly identified and

[10] From this tier, the committee received testimony from Everyone Counts, the Five Cedars Group, Free & Fair, and Democracy Live.

[11] National Conference of State Legislatures, "Voting Equipment," available at: http://www.ncsl.org/research/elections-and-campaigns/voting-equipment.aspx.

[12] Norden, Lawrence and Christopher Famighetti, Brennan Center for Justice, *America's Voting Machines at Risk*, 2015, p. 17, available at: https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.

[13] Most license agreements specify that users maintain the openness of the software they acquire, provide acknowledgement of use in a product, and respect the licenses of components that come from other organizations; some require that modifications also be shared.

corrected) and continuously improves the software base. Since the software itself has only nominal cost, revenue comes from providing support and enhancements. The cost of entry to the provider market is low, enabling competition that tends to drive down costs.[14]

Since 2005, for instance, the Travis County (TX) Clerk has been studying how to improve the security and efficiency of electronic voting systems while making incremental changes in existing processes to anticipate and effectively confront emerging threats. Travis County collaborated with experts in computer science, cryptography and computer security, statistics, and human factor engineering to build a voting system to resolve concerns about electronic voting. That system, STAR Vote (Secure, Transparent, Auditable, Reliable), was designed to offer the speed and accuracy of electronic voting as well as advantages for voters with disabilities. It also provided a paper ballot selection summary for recount and audit purposes.

STAR Vote offered end-to-end-verifiable (E2E-V) elections and included support for risk-limiting audits with enhanced voter privacy. The system would have offered two paper record proofs. One provided a record of a voter's selections. This was deposited into a ballot box at the polling place. The precinct ballot counter matched an electronic copy of the marked ballot stored in the ballot-marking device to the paper record inserted into the ballot box. Ballots with stray marks or those that did not match the electronic version of the ballot were rejected. The second paper record was a receipt with a hash code that the voter retained. Following an election, the voter could access an online bulletin board to verify that the code printed on his or her receipt was included in a list of codes representing all ballots tallied.

A Request for Proposals (RFP) seeking entities to build STAR Vote was issued in late 2016, and proposals were submitted by prospective vendors early in 2017. However, the proposals received were not sufficient to build a complete voting system, and Travis County was unable to pursue the building of STAR Vote.[15]

In 2009, the Los Angeles (LA) County Registrar-Recorder/County Clerk launched the Voting System Assessment Project (VSAP) project when it determined that no system on the market was adequate to meet the needs of the electorate in LA County (the project was later renamed Voting Solutions for All People, as it changed focus from assessment to implementation). The project is working to design and launch a new voting system for the county. The goals of VSAP are to implement publicly owned voting sys-

[14] While the cost of entry to the provider market is low, open-source systems need to be maintained, and this maintenance is typically provided by vendors at a cost.

[15] DeBeauvior, Dana, "STAR Vote – A Change of Plans," September 26, 2017, available at: www.traviscountyelections.org. Ms. DeBeauvoir is a member of the committee that authored the current report.

tems; spur innovation in the voting system market; encourage a regulatory environment that allows for the development, certification, and implementation of publicly owned, voter-centered systems; establish LA County as a new model for voting system development and implementation; and make research findings available for other jurisdictions to utilize and replicate the LA County design process where desired.[16] Currently, VSAP is developing a vote tally system, conducting a vote center placement assessment, and soliciting for system manufacturing and certification.[17]

Prime III is voting software developed at Auburn University in 2003 through a public-private partnership.[18] The system was designed to be "a secure, multimodal electronic voting system that delivers the necessary system security, integrity and user satisfaction safeguards in a user-friendly interface that accommodates all people regardless of ability."[19] Currently, Prime III is the only open-source voting system that has been used in state, federal, and local elections. In 2015, New Hampshire adopted Prime III and renamed it One4All. The One4All system was used in 2016 primaries as well as the presidential election.[20]

In the voting marketplace, the STAR vote proposal, the VSAP project, and the Prime III system are all possible bases for an open-source software base. In this setting, jurisdictions, singly or collectively, would have to assume the costs and time associated with the certification of their open-source voting system.[21]

Public-private partnerships could spark innovation in the voting technology marketplace. Creating a partnership with academia might generate innovations in the voting technology marketplace. The ES&S ExpressVote

[16] Bennett, Kenneth and Monica Flores, County of Los Angeles County (CA) Registrar-Recorder/County Clerk, presentation to the committee, December 7, 2017, Denver, CO.

[17] Circa December 2017. LA County has since indicated that the system will run on an open-source platform as opposed to open-source software. In June 2018, a contract was awarded to Smartmatic to assist the county with the development, manufacturing, and implementation of the system.

[18] The partnership included the National Science Foundation, the U.S. Election Assistance Commission, Auburn University, Clemson University, and the University of Florida. Dr. Juan E. Gilbert, who serves as a member of the committee that authored the current report, was a developer of Prime III.

[19] See http://www.primevotingsystem.com/.

[20] New Hampshire Assistant Secretary of State Tom Manning stated, "The old system required us to pay a little bit less than $250,000 a year in licensing fees for the software that ran in [sic] and then the telephone lines that we needed to connect to our data center would run us about $10,000 a month." See Ganley, Rick and Michael Brindley, "Tablet-Based Ballot System for Blind Voters to Debut During N.H. Primary," New Hampshire Public Radio, February 8, 2016, available at: http://nhpr.org/post/tablet-based-ballot-system-blind-voters-debut-during-nh-primary#stream/0.

[21] See "The Business of Voting: Market Structure and Innovation in the Election Technology Industry," pp. 32-33.

Universal Voting System is an example of a product that resulted from a public-private partnership between ES&S and the Prime III team of academic researchers.

Developing open interfaces between systems can provide opportunities for component-based systems where the components are from different suppliers, and Common Data Formats (CDFs) have been developed to facilitate interoperability. Electronic products used by election officials must be able to share data between devices (or with a common host) if they are to be part of an integrated election administration process. As the "data language" used by such products tends to be proprietary, devices from one manufacturer might not be able to communicate with products from another manufacturer. Election officials may, therefore, need to purchase all their election systems from a single vendor.[22]

The National Institute of Standards and Technology is currently developing a CDF for election systems.[23]

Findings

There is a lack of dedicated funding for new voting systems. Elections funding competes with other state and local programs, and election funding may not receive high priority.

The high cost of maintenance agreements and the bundling of system hardware, software, and services limits election administrators' flexibility with regard to future purchases of voting systems. The expense of purchasing electronic voting systems or purchasing enough extra inventory of paper, optical scan ballots (and resources to secure them) to satisfy the needs of vote centers or early voting programs is not affordable for many local jurisdictions.

Great strides have been made to reform the voting system certification process. Compliance is voluntary and standard setting is difficult, but the efforts of the U.S. Election Assistance Commission and the National Institute of Standards and Technology should be applauded.

A standard national certification process would help to increase competition among voting technology vendors.

The relatively small and underfunded market for voting technology presents an obstacle for new entrants and may inhibit the use of the latest devices in election administration.

[22] National Institute of Standards and Technology, "An Introduction to the Common Data Format Project," available at: https://collaborate.nist.gov/voting/bin/view/Voting/WhyIsACDFNeeded.

[23] See National Institute of Standards and Technology, "The NIST Interoperability Public Working Group and Common Data Format (CDF) for Election Systems Project," available at: https://www.nist.gov/itl/voting/interoperability.

The structure of the current election technology marketplace provides limited incentives for technological innovation.

There are alternatives to the current private-sector, for-profit marketplace for election systems.

RECOMMENDATIONS

6.4 Congress should:

a. create incentive programs for public-private partnerships to develop modern election technology;

b. appropriate funds for distribution by the U.S. Election Assistance Commission for the ongoing modernization of election systems; and

c. authorize and appropriate funds to the National Institute of Standards and Technology to establish Common Data Formats for auditing, voter registration, and other election systems.

6.5 Along with Congress, states should allocate funds for the modernization of election systems.

6.6 The U.S. Election Assistance Commission and the National Institute of Standards and Technology should continue to collaborate on changes to the certification process that encourage the modernization of voting systems.

6.7 The National Institute of Standards and Technology should complete the Common Data Format standard for election systems.

6.8 New election systems should conform to the Common Data Format standard developed by the National Institute of Standards and Technology.

THE FEDERAL ROLE

Overview and Analysis

As noted in previous chapters, elections in the United States are administered in a decentralized fashion. States and local jurisdictions carry out the primary functions and processes associated with federal and state elections. States and local jurisdictions, consequently, assume responsibility for the majority of expenses associated with election administration.

The federal government has, however, a legitimate role to play in election administration. The U.S. Constitution gives the federal government ample authority to regulate elections, and over the past 50 years, Congress has exercised federal authority in many contexts. The Elections Clause (Article I, Section 4, Clause 1) of the Constitution specifies that the states will determine the "Times, Places, and Manner" of congressional elections, and allows Congress to "make or alter" states' regulations. Moreover, each amendment to the Constitution that prevents discrimination in voting rights—the 15th Amendment (race), the 19th Amendment (sex), the 24th Amendment (poll taxes), the 26th Amendment (age)—grants Congress the power "to enforce this article by appropriate legislation." Likewise, the 14th Amendment, which the Supreme Court has interpreted to provide protection for voting rights even for groups beyond those specifically enumerated by those other amendments and to protect against other undue burdens on the right to vote, contains similar enforcement provisions.

Congress has exercised its constitutional authority to regulate elections in a range of contexts. One of the earliest pieces of election-related legislation was passed by Congress in 1842. It required that each representative be elected by a separate district. [24] Soon after, in 1845, Congress chose a single date for all national elections—the first Tuesday after the first Monday in November.[25] As discussed in Chapter 4 (see pp. 55-56), Congress has used its authority to regulate the mechanics of elections ever since.

The federal role in elections has increased over time in response to issues of national concern. With each effort for greater national uniformity in elections or federal voting rights protection, concerns about localism and state sovereignty are raised. Elections continue to be administered by states and localities, often against a backdrop of federal regulations that ensure protection of voting rights. Nevertheless, great variation exists among states in certain basic components of the electoral process. This diversity is a double-edged sword. On the one hand, the quality of election administration can vary based on where a voter lives. On the other, the lack of a single national voting system may offer some protection against widespread compromise of the results of an election. That limited protection may be negated, however, when attackers can use comprehensive data analysis to target voting jurisdictions that can change the outcome of an election.[26]

When exercising federal authority, the government has recognized that, while election administration is primarily a state and local responsibility, there are occasions where the federal government should play a leading role by providing resources that will nudge election administrators in certain

[24] The Act, the Apportionment Act of 1842, states that, "in every case where a State is entitled to more than one Representative, the number to which each State shall be entitled under this apportionment shall be elected by districts, composed of contiguous territory, equal in number to the number of Representatives to which said State may be entitled; no one district electing more than one Representative."

[25] Prior to this time, Congress allowed states to conduct presidential elections at any point in the 34 days before the first Wednesday in December—the meeting of the state electoral colleges.

[26] Potential attackers could use such data to target those jurisdictions that are deemed easiest to compromise.

directions (e.g., to upgrade election technology) or that will provide access to intelligence information pertinent to national security.

The federal government also has a role to play in ensuring the resilience of the nation in the face of cyberattacks. As noted throughout this report, protecting America's election infrastructure became a national security concern in the wake of Russian cyber efforts to target U.S. voting databases and systems. These efforts prompted the federal government, through the U.S. Department of Homeland Security (DHS), to designate election infrastructure as a subsector of the existing Government Facilities critical infrastructure sector, placing it on par with sectors such as banking and electricity. This designation prioritized for the first time the protection of election systems as a national security issue, identified DHS as the lead federal agency to coordinate with state and local officials, and provided states with access to government national security information.

The critical infrastructure designation was met with resistance in the elections community. Immediately after the nation's election systems were given critical infrastructure status, the National Association of Secretaries of State (NASS) issued a statement wherein it asserted that

> No credible evidence of hacking, including attempted hacking of voting machines or vote counting, was ever presented or discovered in any state. State and local autonomy over elections is our greatest asset against malicious cyberattacks and manipulation. Our decentralized, low-connectivity electoral process is inherently designed to withstand such threats.

"While we recognize," the statement continued, "the need to share information on threats and risk mitigation in our elections at all levels of government, as we did throughout the 2016 cycle, it is unclear why a critical infrastructure classification is now necessary for this purpose."[27] NASS provides further clarification on its website:

> While NASS members recognize the need to share information on threats and risk mitigation in our elections at all levels of government, Secretaries of State oppose the critical infrastructure designation based on the federal government's continued lack of transparency and clarity with chief state election officials on plans for implementing the designation.[28]

However, the critical infrastructure designation only allows DHS to provide support to "the private sector and state, local, tribal, and territorial

[27] National Association of Secretaries of State, "NASS Statement on Critical Infrastructure Designation for Elections," January 9, 2017, available at: https://www.nass.org/node/228.

[28] National Association of Secretaries of State, "Elections as Critical Infrastructure: What Does It Mean?," available at: https://www.nass.org/initiatives/election-cybersecurity.

governments in the management of their cyber risk" and "provide technical assistance in the event of a cyber incident, as requested." The department can provide (1) "automated, recurring scans of Internet facing systems that provide the perspective of the vulnerabilities and configuration errors that a potential adversary could see;" (2) "penetration testing, social engineering, wireless access discovery, database scanning, and operating system scanning;" (3) "alerts, analysis reports, bulletins, best practices, cyber threat indicators, guidance, points-of-contact, security tips, and technical documents to stakeholders;" (4) "regionally located personnel who engage state and local governments, election crime coordinators, and vendors to offer immediate and sustained assistance, coordination, and outreach to prepare and protect from cyber and physical threats;" and (5) access to "cybersecurity operations centers that maintain close coordination among the private sector, government officials, the intelligence community, and law enforcement to provide situational awareness and incident response, as appropriate."[29]

As discussed in Chapter 1, Congress created the EAC to serve as a clearinghouse for election administration research and information and to award federal funds to allow states to replace antiquated voting systems and to improve election administration. A full commission has four members, and currently there are two vacancies. Importantly, any action of the Commission authorized by HAVA requires approval of at least three of its members. Federal funding for the EAC is currently less than $10 million/year and includes funds for transfer to the National Institute of Standards and Technology for election reform administration activities.

Although there are strong efforts by research groups and nonprofit organizations to gather data to inform election-related decisions and legislation, additional work is needed. The federal government has a role in sponsoring (1) research that distinguishes beliefs about election issues from evidence-based understanding; and (2) pilot programs to explore novel solutions to problems identified in Chapters 4 and 5. Broad statistics on voting patterns, the effect of by-mail voting, the effect of various factors on voter turnout, and other questions need to be refined to reflect particular regions and socioeconomic factors. The influence of technological advances such as machine learning and data mining on the elections system needs to be better understood. Though the conduct of elections is largely delegated to the states, the federal government has a responsibility to sponsor research that protects the integrity of elections.

[29] Hale, Geoffrey, U.S. Department of Homeland Security, presentation to the committee (Slides 4 and 7), April 4, 2017, Washington, DC, available at: http://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_178365.pdf.

Findings

There is no centralized election body that establishes rules for national elections or reports the results of national elections.

The decentralized character of U.S. election administration provides a check against a widespread technological breakdown or cyberattack. At the same time, it increases the number of potential vectors of attack against election administration, many of which are small jurisdictions that are under-resourced to respond adequately to modern cyber-risks.

The range and heterogeneity of local statutes and election administration challenges prevent implementation of a single uniform voting system across the country.

There is no central location wherein problems (e.g., long lines, malfunctioning machines, etc.) arising on Election Day are reported, compiled, and analyzed.

The federal government has increased its involvement in the administration of national elections in response to serious system concerns.

While funds allocated under HAVA were critical to the improvement of elections, without sustained federal funding, jurisdictions may be unable to purchase equipment that is easy to use, accessible, secure, and reliable.

The nature of threats to election systems is changing as state and non-state actors attempt to undermine election systems through cyber and information warfare.

Addressing foreign government assaults on election databases and systems require new approaches and better federal-state collaboration. States and local governments do not have an independent ability to protect election infrastructure against nation-state attacks.

The designation by DHS of election systems as a subsector of the existing government facilities critical infrastructure sector is correct and appropriate. This designation reflects appropriately the need for sophisticated technical expertise and sharing of intelligence information required to protect the nation's election infrastructure.

The EAC has a vital role to play in improving election administration.

The federal government has an important role to play in understanding the impact of technological changes on the conduct of elections and in evaluating possible remedies to election threats.

RECOMMENDATION

6.9 To improve the overall performance of the election process:

a. The president should nominate and Congress should confirm a full U.S. Election Assistance Commission and ensure that the U.S. Election Assistance Commission has sufficient members to sustain a quorum.

b. Congress should fully fund the U.S. Election Assistance Commission to carry out its existing functions.

c. Congress should require state and local election officials to provide the U.S. Election Assistance Commission with data on voting system failures during elections as well as information on other difficulties arising during elections (e.g., long lines, fraudulent voting, intrusions into voter registration databases, etc.). This information should be publicly available.

7

Securing the Future of Voting

As this report illustrates, voting in the United States is a complicated process that involves multiple levels of government, personnel with a variety of skills and capabilities, and numerous electronic systems that interact in the performance of a multitude of tasks. Unfortunately, our current system is vulnerable to internal and external threats.

As the U.S. elections system has undergone significant technological changes and adapted to meet changing needs, the American electorate has largely remained confident that the ballots it casts are accurately counted and tabulated. Nevertheless, recent events make it clear that our system of voting must evolve in order to also protect against external actors who wish to undermine confidence in democratic institutions. The new foreign threat has profound implications for the future of voting and obliges us to seriously reexamine both the conduct of elections in the United States and the role of federal and state governments in securing our elections. We must think strategically and creatively about the administration of U.S. elections. We must confront barriers (both real and perceived) that inhibit partnerships that would facilitate reliable, accessible, verifiable, and secure voting. We must foster an environment that promotes innovation in election systems technology, provides election administrators with human resource tools to increase the professionalization of the election workforce, allocates appropriate resources for the operation of elections, and better secures elections by developing auditing tools that provide assurances that ballots cast are counted and tabulated correctly and that the results of elections are accurate.

We have witnessed tremendous technological advances in recent decades, but we must give careful consideration to the adoption of technologies that might increase convenience for voters. We do not, at present, have the technology to offer a secure method to support Internet voting. It is certainly possible that individuals will be able to vote via the Internet in the future, but technical concerns preclude the possibility of doing so securely at present. It is difficult to secure the electronic systems used in voting even now. In systems ranging from electronic voter registration databases and electronic pollbooks to voting systems, corresponding physical records are essential for matching purposes. Furthermore, election administrators must have the capacity to conduct routine audits on their electronic systems throughout the election process.

To fully address the challenges inherent in electronic election systems and to prevent foreign interference, federal, state, and local officials must adopt innovative measures to ensure that the results of elections reflect the will of the electorate. Election systems in the future must be not only secure but also adaptive and resilient. To ensure the integrity of the voting process, we must be constantly vigilant, have the ability to verify and safeguard data, make continuous improvements in voting processes and technologies, and, through engagement and transparency, consistently educate and reassure our electorate. If the challenges currently facing our election systems are ignored, we risk an erosion of confidence in our elections system and in the integrity of our election processes.

THE ROLE OF THE U.S. ELECTION ASSISTANCE COMMISSION AND FEDERAL AGENCIES

The U.S. Election Assistance Commission (EAC) performs an important role in U.S. elections by serving as a clearinghouse for information on election administration, establishing voting system guidelines, accrediting testing laboratories, certifying voting systems, and overseeing the disbursement of funds for the improvement of elections. Each of these functions enhances the conduct of elections. To perform these functions properly, the EAC depends on adequate funding and resources.

The National Institute of Standards and Technology (NIST) assists the EAC by providing critical technical expertise. Working together, NIST and the EAC have made numerous contributions to the improvement of electronic voting systems. However, as this report indicates, there are many technical obstacles to overcome if electronic voting systems are to be secured from external and internal threats.

Other federal agencies, such as the National Science Foundation and the U.S. Department of Defense, have, through their research programs, made positive contributions to our understanding of elections and election administration.

RECOMMENDATIONS

7.1 Congress should provide appropriate funding to the U.S. Election Assistance Commission to carry out the functions assigned to it in the Help America Vote Act of 2002 as well as those articulated in this report.

7.2 Congress should authorize and provide appropriate funding to the National Institute of Standards and Technology to carry out its current elections-related functions and to perform the additional functions articulated in this report.

7.3 Congress should authorize and fund immediately a major initiative on voting that supports basic, applied, and translational research relevant to the administration, conduct, and performance of elections. This initiative should include academic centers to foster collaboration both across disciplines and with state and local election officials and industry.

The U.S. Election Assistance Commission, National Institute of Standards and Technology, U.S. Department of Homeland Security, National Science Foundation, and U.S. Department of Defense should sponsor research to:

- determine means for providing voters with the ability to easily check whether a ballot sent by mail has been dispatched to him or her and, subsequently, whether his or her marked ballot has been received and accepted by the appropriate elections officials;
- evaluate the reliability of various approaches (e.g., signature, biometric, etc.) to voter authentication;
- explore options for testing the usability and comprehensibility of ballot designs created within tight, pre-election timeframes;
- understand the effects of coercion, vote buying, theft, etc., especially among disadvantaged groups, on voting by mail and to devise technologies for reducing this threat;
- determine voter practices regarding the verification of ballot marking device–generated ballots and the likelihood of voters, both with and without disabilities, will recognize errors or omissions;
- assess the potential benefits and risks of Internet voting;
- evaluate end-to-end-verifiable election systems in various election scenarios and assess the potential utility of such systems for Internet voting; and
- address any other issues that arise concerning the integrity of U.S. elections.

CONCLUSION

As a nation, we have the capacity to build an elections system for the future, but doing so requires focused attention from citizens, federal, state, and local governments, election administrators, and innovators in academia and industry. It also requires a commitment of appropriate resources. Representative democracy only works if all eligible citizens can participate in elections, have their ballots accurately cast, counted, and tabulated, and be confident that their ballots have been accurately cast, counted, and tabulated.

Appendixes

Appendix A

Biographical Information of Committee and Staff

CO-CHAIRS

LEE C. BOLLINGER has served as the president of Columbia University since 2002 and is the longest serving Ivy League president. He is Columbia's first Seth Low Professor of the University, a member of the Columbia Law School faculty, and one of the country's foremost First Amendment scholars. His book, *The Free Speech Century*, co-edited with Geoffrey R. Stone, will be published in the fall of 2018 by Oxford University Press.

From 1996 to 2002, Bollinger was the president of the University of Michigan at Ann Arbor. He led the school's litigation in *Grutter v. Bollinger* and *Gratz v. Bollinger*, resulting in Supreme Court decisions that upheld and clarified the importance of diversity as a compelling justification for affirmative action in higher education. He speaks and writes frequently about the value of racial, cultural, and socio-economic diversity to American society through opinion columns, media interviews, and public appearances.

Bollinger received his Juris Doctor from Columbia Law School. He served as a law clerk to Judge Wilfred Feinberg of the United States Court of Appeals for the Second Circuit and Chief Justice Warren Burger of the Supreme Court. Bollinger went on to join the faculty of the University of Michigan Law School in 1973, becoming dean of the school in 1987. He became provost of Dartmouth College in 1994 before returning to the University of Michigan in 1996 as president.

MICHAEL A. McROBBIE is the 18th president of Indiana University (IU). Dr. McRobbie joined IU in 1997 as vice president for information technology and chief information officer, and was appointed vice president for research in 2003. He was named interim provost and vice president for academic affairs for Indiana University's Bloomington campus in 2006 and became president the following year. He is now one of the longest serving public university presidents in the Association of American Universities.

As president, McRobbie has led the largest ever academic restructuring and expansion of IU, with the establishment of 10 new schools, over $2.5 billion of new construction, and the establishment of the university's Global Gateway Network of offices around the world.

As chief information officer, McRobbie was responsible for a number of initiatives of national importance, including the establishment of the Global Network Operations Center, now responsible for the operation and management of over 20 national and international research and education networks including the Internet2 network, the National Oceanic and Atmospheric Administration's research network, and international connections to major research and education networks in the Asia-Pacific, Europe and Africa, and the establishment of the Research and Education Network Information Sharing and Analysis Center (REN-ISAC) focused on network based cybersecurity issues for its 540 national and international members —the only ISAC in higher education.

McRobbie holds faculty appointments in computer science, philosophy, and cognitive science and informatics and has been an active researcher in information technology and logic over the course of his career. He is a fellow of the American Academy of Arts and Sciences, an honorary fellow of the Australian Academy of Humanities and a member of the Council on Foreign Relations. He was awarded the Sagamore of the Wabash by the governor of Indiana in 2007 and 2017. McRobbie's commitment to international engagement in higher education has been recognized through the receipt of the International Citizen of the Year award in Indiana and five honorary degrees from foreign universities. A native of Australia, in 2010 he was made an Officer of the Order of Australia, Australia's national honors system.

MEMBERS

ANDREW W. APPEL is the Eugene Higgins Professor of Computer Science at Princeton University, where he has been on the faculty since 1986. He served as department chair from 2009 to 2015. His research is in software verification, computer security, programming languages and compilers, and technology policy. He received his A.B. summa cum laude in physics from Princeton in 1981 and his Ph.D. in computer science from Carnegie

Mellon University in 1985. He has been editor-in-chief of *ACM Transactions on Programming Languages and Systems* and is a fellow of the ACM (Association for Computing Machinery). He has worked on fast N-body algorithms (1980s), Standard ML of New Jersey (1990s), Foundational Proof-Carrying Code (2000s), and the Verified Software Toolchain (2010s). He is the author of several scientific papers on voting machines and election technology, served as an expert witness on two voting-related court cases in New Jersey, and has taught a course at Princeton on election machinery.

JOSH BENALOH is senior cryptographer at Microsoft Research and an affiliate faculty member in the University of Washington School of Computer Science and Engineering. He holds an S.B. in mathematics from Massachusetts Institute of Technology and M.S., M. Phil., and Ph.D. degrees in computer science from Yale University where his 1987 doctoral dissertation "Verifiable Secret-Ballot Elections" introduced the use of homomorphic encryption as a paradigm to enable election tallies to be verified by individual voters and observers without having to trust election equipment, vendors, or personnel.

Benaloh served for 17 years as a director of the International Association for Cryptologic Research, and he currently serves on the Coordinating Committee of the Election Verification Network. He has published and spoken extensively on cryptography, policy, and election technologies and is an author of the widely covered 2015 "Keys Under Doormats" report, which explores the technical implications of restrictions on cryptography and has influenced the ongoing political debate. Benaloh is also an author of the 2015 U.S. Vote Foundation report on the viability of end-to-end-verifiable Internet voting systems. Outside of elections, policy, and technology, Benaloh recently completed 2 years as chair of the Sound Transit Citizen Oversight Panel, which oversees the Seattle regional transit authority that is currently investing billions annually on new infrastructure in the Puget Sound region.

KAREN COOK is the Ray Lyman Wilbur Professor of Sociology and vice provost for Faculty Development and Diversity at Stanford University. She is also the director of the Institute for Research in the Social Sciences (IRiSS) at Stanford and a trustee of the Russell Sage Foundation. Cook has a long-standing interest in social exchange, social networks, social justice, and trust in social relations. She has edited a number of books in the Russell Sage Foundation Trust Series including *Trust in Society* (2001), *Trust and Distrust in Organizations: Emerging Perspectives* (with R. Kramer, 2004), *eTrust: Forming Relations in the Online World* (with C. Snijders, V. Buskens, and Coye Cheshire, 2009), and *Whom Can Your Trust?* (with M. Levi and R. Hardin, 2009). She is co-author of *Cooperation without*

Trust? (with R. Hardin and M. Levi, 2005). In 1996, she was elected to the American Academy of Arts and Sciences and in 2007 to the National Academy of Sciences. In 2004 she received the ASA Social Psychology Section Cooley Mead Award for Career Contributions to Social Psychology.

DANA DeBEAUVOIR is in her 31st year serving as the elected Travis County Clerk in Austin, Texas. The Clerk's Office has a wide range of responsibilities including conducting elections; filing and preserving real property records; issuing marriage licenses; and managing civil, misdemeanor, and probate court records. With the passage of the Help America Vote Act in 2002, DeBeauvoir assumed new duties for the more than 130 local jurisdictions conducting their elections jointly with Travis County. She currently serves as the Texas representative on the federal Election Assistance Commission Standards Board, having served in that role since the position was established.

DeBeauvoir served as a United Nations Elections Observer at the 1994 election in South Africa that marked the end of apartheid. She served with the International Foundation for Electoral Systems as a consultant preparing for elections in Bangladesh (1995), Sarajevo, Bosnia (1996), and Pristina, Kosovo (1999). She also served as the Legislative Committee Chair for Elections for the County and District Clerks Association from 1995 to 2015. Her first award for improved management, a National Director's Award, presented by the International Association of Clerks, Recorders, Elections Officials, and Treasurers for creating a database of civil case names to cure an inherited and troublesome court backlog, was received in 1989. DeBeauvoir was awarded the 2009 Public Official of the Year by the National Association of County Recorders, Election Officials, and Clerks. The same year, she received the 2009 Minute Man Award for developing improved security practices by The Election Center. In 2014, she received the prestigious Eagle Award from The Election Center.

DeBeauvoir is a graduate of the University of Texas at Arlington, having received a B.A. in sociology/social work in 1979. She received a masters of public affairs in 1981 from the LBJ School of Public Affairs at the University of Texas at Austin. In 2002, she received the LBJ School Alumni Association Distinguished Public Service Award.

MOON DUCHIN is an associate professor in the Department of Mathematics and serves as founding director of the interdisciplinary Program in Science, Technology, and Society at Tufts University. Her mathematical research is in low-dimensional topology, geometric group theory, and dynamics. She leads a research team called the Metric Geometry and Gerrymandering Group (MGGG) that studies novel applications of geometry and topology to redistricting problems. One of the first public activities of the MGGG was a summer school in August 2017 that brought together scholars from law, civil rights, and mathematics to train expert witnesses for voting rights cases. Duchin is a fellow of the American Mathematical Society and holds a CAREER award from the National Science Foundation to study geometry at the intermediate scale between metric spaces and their asymptotic limits. She has lectured widely in pure mathematics and has spoken on the geometry of redistricting to audiences from high schools to a rabbinical school to the Distinguished Lecture Series of the Mathematical Association of America. She holds a Ph.D. in mathematics from the University of Chicago and a B.A. in mathematics and women's studies from Harvard University.

JUAN E. GILBERT is the Andrew Banks Family Preeminence Endowed Professor and chair of the Computer & Information Science & Engineering Department at the University of Florida where he leads the Human Experience Research Lab. He is also a fellow of the American Association of the Advancement of Science, a fellow of the National Academy of Inventors, an Association for Computing Machinery Distinguished Scientist, and a senior member of the Institue of Electrical and Electronics Engineers. Gilbert is the inventor of Prime III, an open-source, secure, and accessible voting technology that has been used in numerous organization elections and recently in statewide elections in New Hampshire.

SUSAN L. GRAHAM is the Pehong Chen Distinguished Professor of Electrical Engineering and Computer Science Emerita at the University of California, Berkeley. She received an A.B. in mathematics from Harvard University and M.S. and Ph.D. degrees in computer science from Stanford University. Her research has spanned programming language design and implementation, software tools, software development environments, and high-performance computing. She was the founding editor-in-chief of the Association for Computing Machinery (ACM) *Transactions on Programming Languages and Systems*. She is a fellow of the ACM, the Institute of Electrical and Electronics Engineers, and the American Academy of Arts and Sciences, and a member of the National Academy of Engineering.

Graham has served on numerous advisory and visiting committees and has been a consultant to a variety of companies. She was a member of the President's Information Technology Advisory Committee from 1997 to 2003. She served as the chief computer scientist for the National Partnership for Advanced Computational Infrastructure from 1997 to 2005. She was a member of the Harvard Board of Overseers from 2001 to 2007 and was president in 2006-2007. Graham was a founding member of the Computing Research Association's Computing Community Consortium, serving first as vice-chair and then as chair. From 2013 to January 2017 she was a member of the President's Council of Advisors on Science and Technology where she co-chaired their study and report "Big Data and Privacy: A Technological Perspective." She is a member of the Harvard Corporation (formally, a fellow of Harvard College).

NEAL KELLEY is registrar of voters for Orange County, California, the fifth largest voting jurisdiction in the United States, serving more than 1.6 million registered voters.

Kelley joined the county as chief deputy registrar of voters in 2004. In his role as the county's chief election official, he leads an organization responsible for conducting elections, verifying petitions, and maintaining voter records.

Prior to joining Orange County, Kelley developed and grew several companies of his own, employing hundreds of people from 1989 to 2004. He was also an adjunct professor with Riverside Community College's Business Administration Department, and served as a police officer in Southern California during the mid-1980s.

In 2009, Kelley earned professional election certification through the national Election Center and Auburn University as a Certified Elections and Registration Administrator. He has been the recipient of several awards for election administration, including recognition from the California State Association of Counties, The Election Center, and the National Association of Counties. He was recently honored with the "2015 Public Official of the Year" from the National Association of County Recorders, Election Officials and Clerks.

Kelley is an appointed member of the U.S. Election Assistance Commission Board of Advisors (and currently serves as chairman) and its Voting Systems Standards Board, is the past president of the California Association of Clerks and Election Officials, and is the immediate past president for the National Association of County Recorders, Election Officials, and Clerks.

Kelley earned a B.S. in business and management from the University of Redlands and an M.B.A. from the University of Southern California.

KEVIN J. KENNEDY left government service on June 29, 2016, with the dissolution of the Wisconsin Government Accountability Board. He presently consults and speaks on issues and topics related to campaign finance, elections, and ethics.

Kennedy served as director and General Counsel for the Wisconsin Government Accountability Board (G.A.B.) from November 5, 2007, through June 29, 2016. Before assuming the top staff position for the G.A.B., he was executive director—and before that legal counsel—for the Wisconsin State Elections Board.

Kennedy served as Wisconsin's chief election official from August 17, 1983 until June 29, 2016. No other individual has served longer in that capacity. Under his leadership, Wisconsin has been consistently recognized as a leader and innovator in the administration of elections, lobbying, and campaign finance.

In addition to his service to the people of Wisconsin, Kennedy has been active in a number of professional organizations. He has testified before Congress, several federal and state legislative bodies, and numerous private organizations active in the fields of campaign finance, elections, ethics, and lobbying.

NATHANIEL PERSILY is the James B. McClatchy Professor of Law at Stanford Law School, with appointments in the departments of Political Science and Communication. Prior to joining Stanford, Persily taught at Columbia and the University of Pennsylvania Law School, and as a visiting professor at Harvard, New York University, Princeton, the University of Amsterdam, and the University of Melbourne. Persily's scholarship and legal practice focus on American election law or what is sometimes called the "law of democracy," which addresses issues such as voting rights, political parties, campaign finance, redistricting, and election administration. He has served as a special master or court-appointed expert to craft congressional or legislative districting plans for Georgia, Maryland, Connecticut, and New York, and as the senior research director for the Presidential Commission on Election Administration. In addition to dozens of articles (many of which have been cited by the Supreme Court) on the legal regulation of political parties, issues surrounding the census and redistricting process, voting rights, and campaign finance reform. Persily is also coauthor of the leading election law casebook, *The Law of Democracy* (Foundation Press, 5th ed., 2016), with Samuel Issacharoff, Pamela Karlan, and Richard Pildes. His current work, for which he has been honored as an Andrew Carnegie Fellow, examines the impact of changing technology on political communication, campaigns, and election administration. He has edited several books, including *Public Opinion and Constitutional Controversy* (Oxford Press, 2008); *The Health Care Case: The Supreme Court's Decision and Its Implications* (Oxford Press 2013); and *Solutions to Political Polarization in America* (Cambridge Press, 2015). He received a B.A. and M.A. in political science from Yale (1992); a J.D. from Stanford (1998) where he was president of the *Stanford Law Review*; and a Ph.D. in political science from University of California, Berkeley in 2002.

RONALD L. RIVEST is an institute professor in the Massachusetts Institute of Technology's (MIT) Department of Electrical Engineering and Computer Science, and a leader of the Cryptography and Information Security research group within MIT's Computer Science and Artificial

Intelligence Laboratory. He received a B.A. in mathematics from Yale University in 1969 and a Ph.D. in computer science from Stanford University in 1974.

Rivest is a fellow of the Association for Computing Machinery and of the American Academy of Arts and Sciences and a member of the National Academy of Engineering and the National Academy of Sciences.

Rivest is an inventor of the RSA public-key cryptosystem and a founder of RSA Data Security. He has extensive experience in cryptographic design and cryptanalysis, and he has published numerous papers in these areas. He has served as director of the International Association for Cryptologic Research, the organizing body for the Eurocrypt and Crypto conferences, and of the Financial Cryptography Association. He has also worked extensively in the areas of computer algorithms and machine learning.

Rivest is a member of the CalTech/MIT Voting Technology Project and serves on the Board of Verified Voting. He has served on the TGDC (Technical Guidelines Development Committee) that advises the U.S. Election Assistance Commission and chaired the committee's subgroup on Security and Transparency.

CHARLES STEWART III is the Kenan Sahin Distinguished Professor of Political Science at the Massachusetts Institute of Technology (MIT), where he has taught since 1985, and a fellow of the American Academy of Arts and Sciences. His research and teaching areas include elections, congressional politics, and American political development.

Since 2001, Stewart has been a member of the Caltech/MIT Voting Technology Project, a leading research effort that applies scientific analysis to questions about election technology, election administration, and election reform. He is currently the MIT director of the project. In addition, he is the director of the MIT Election Data and Science Lab, a new initiative to disseminate scientific analysis of election processes among academic researchers and election practitioners. Stewart is an established leader in the analysis of the performance of election systems and the quantitative assessment of election performance. Working with the Pew Charitable Trusts, he helped with the development of Pew's Elections Performance Index. Stewart also provided advice to the Presidential Commission on Election Administration. His research on measuring the performance of elections and polling place operations is funded by Pew, the Democracy Fund, and the Hewlett Foundation. He recently published *The Measure of American Elections* (2014 with Barry C. Burden).

His current research about Congress touches on the historical development of committees, origins of partisan polarization, and Senate elections. His recent books of congressional research include *Electing the Senate*

(2014 with Wendy J. Schiller), *Fighting for the Speakership* (2012 with Jeffery A. Jenkins), and *Analyzing Congress* (2nd ed., 2011).

Stewart has been recognized at MIT for his undergraduate teaching, being named to the second class of MacVicar Fellows in 1994, awarded the Baker Award for Excellence in Undergraduate Teaching, and the recipient of the Class of 1960 Fellowship. From 1992 to 2015, he served as Head of House of McCormick Hall, along with his spouse, Kathryn M. Hess.

Stewart received his B.A. in political science from Emory University and S.M. and Ph.D. from Stanford University.

STAFF

ANNE-MARIE MAZZA, Ph.D., is the senior director of the Committee on Science, Technology, and Law. Mazza joined the National Academies of Sciences, Engineering, and Medicine in 1995. In 1999 she was named the first director of the Committee on Science, Technology, and Law. Mazza has been the study director on numerous National Academies' activities involving emerging technologies (e.g., human genome editing and synthetic biology), science in the courtroom (e.g., eyewitness identification and forensic science), and laws and regulations related to the governance of academic research (e.g., with regard to dual use research of concern, intellectual property, and human subjects). Between October 1999 and October 2000, Mazza divided her time between the National Academies and the White House Office of Science and Technology Policy, where she served as a senior policy analyst responsible for issues associated with a Presidential Review Directive on the government-university research partnership. Before joining the National Academies, Mazza was a senior consultant with Resource Planning Corporation. She is a fellow of the American Association for the Advancement of Science. Mazza was awarded a B.A., M.A., and Ph.D. from The George Washington University.

JON EISENBERG is the senior board director of the Computer Science and Telecommunications Board of the National Academies of Sciences, Engineering, and Medicine. He has been study director for a diverse body of work, including a series of studies exploring Internet and broadband policy and networking and communications technologies. In 1995-1997 he was an American Association for the Advancement of Science, Engineering, and Diplomacy Fellow at the U.S. Agency for International Development, where he worked on technology transfer and information and telecommunications policy issues. Eisenberg received his Ph.D. in physics from the University of Washington in 1996 and B.S. in physics with honors from the University of Massachusetts at Amherst in 1988.

STEVEN KENDALL is program officer for the Committee on Science, Technology, and Law. Dr. Kendall has contributed to numerous National Academies of Sciences, Engineering, and Medicine reports, including *Dual Use Research of Concern in the Life Sciences: Current Issues and Controversies* (2017); *Optimizing the Nation's Investment in Academic Research* (2016); *International Summit on Human Gene Editing: A Global Discussion* (2015); *Identifying the Culprit: Assessing Eyewitness Identification* (2014); *Positioning Synthetic Biology to Meet the Challenges of the 21st Century* (2013); the *Reference Manual on Scientific Evidence*, 3rd Edition (2011); *Review of the Scientific Approaches Used During the FBI's Investigation of the 2001 Anthrax Mailings* (2011); *Managing University Intellectual Property in the Public Interest* (2010); and *Strengthening Forensic Science in the United States: A Path Forward* (2009). Kendall completed his Ph.D. in the Department of the History of Art and Architecture at the University of California, Santa Barbara, where he wrote a dissertation on 19th century British painting. Kendall received his M.A. in Victorian art and architecture at the University of London. Prior to joining the National Research Council in 2007, he worked at the Smithsonian American Art Museum and The Huntington in San Marino, California.

KAROLINA KONARZEWSKA is program coordinator for the Committee on Science, Technology, and Law. She holds a master's degree in applied economics from George Mason University, a master's degree in international relations from New York University, and a bachelor's degree in political science from the College of Staten Island, City University of New York. Prior to joining the National Academies of Sciences, Engineering, and Medicine, she worked at various research institutions in Washington, DC, where she covered political and economic issues pertaining to Europe, Russia, and Eurasia.

WILLIAM J. SKANE is former executive director of the Office of News and Public Information at the National Academies of Sciences, Engineering, and Medicine. He retired in 2017, having assumed the position in 2002. Before joining the Academies, Skane was the Washington producer for the CBS News broadcast *Sunday Morning with Charles Kuralt* (1991-2002) and national medical producer for the *CBS Evening News with Dan Rather* (1984-1991). He is the recipient of three Emmy awards, two Peabody awards, a Sigma Delta Chi award for breaking news coverage, and the Westinghouse-AAAS award for science reporting on television. Skane began his journalism career as the science reporter for public television station KQED in San Francisco. He earned an Honors B.A. in economics from Stanford University, an M.J. from the Graduate School of Journalism at the University of California, Berkeley, and an M.Ed. from The George Washington University.

Appendix B

Committee Meeting Agendas

Meeting 1
Washington, DC
April 4-5, 2017

TUESDAY, APRIL 4, 2017

OPEN SESSION

10:00 AM Welcome/Introductions/Meeting Overview

Committee Co-Chairs:

Lee C. Bollinger, Columbia University
Michael A. McRobbie, Indiana University

10:15 AM Hand-off of Study from Co-Chairs of Committee on Science, Technology, and Law

Speakers:

David Baltimore, California Institute of Technology
David S. Tatel, U.S. Court of Appeals for the District of Columbia Circuit

10:30 AM Charge to the Committee

Speaker:

Geri Mannion, Carnegie Corporation of New York

10:45 AM Overview of the U.S. Election Process

Speaker:

Thad Hall, Fors Marsh Group

11:15 AM Q&A with Committee

12 noon Lunch

1:00 PM Overview of Voting Technologies

Speakers:

Brian Newby and Jessica Myers, U.S. Election Assistance Commission

1:20 PM Q&A with Committee

2:00 PM Voting Equipment as a Critical National Infrastructure

Speaker:

Geoffrey Hale, U.S. Department of Homeland Security

2:20 PM Q&A with Committee

3:00 PM Break

3:15 PM Issues Arising from the 2016 Presidential Election

Speaker:

Alex Padilla, National Association of Secretaries of State

3:35 PM Q&A with Committee

4:10 PM The View of Elections at the Local Level

Speaker:

David Stafford, Escambia County, FL

4:30 PM Q&A with Committee

5:00 PM Adjourn to Closed Session

WEDNESDAY, APRIL 5, 2017

OPEN SESSION

10:00 AM 2014 Report and Recommendations of the Presidential Commission on Election Administration

Speaker:

Robert F. Bauer, Perkins Coie LLP

10:20 AM Q&A with Committee

11:00 AM Challenges Ahead: View from the U.S. Election Assistance Commission

Speaker:

Matthew Masterson, U.S. Election Assistance Commission

11:20 AM Q&A with Committee

12 noon Adjourn to Closed Session

Meeting 2
New York, NY
June 12-13, 2017

MONDAY, JUNE 12, 2017

OPEN SESSION

10:00 AM Welcome/Introductions/Meeting Overview

Committee Co-Chairs:

Lee C. Bollinger, Columbia University
Michael A. McRobbie, Indiana University

10:10 AM Increasing Vulnerability: Security Challenges

Speakers:

J. Alex Halderman, University of Michigan
Alexander Schwarzmann, University of Connecticut

10:45 AM Q&A with Committee

11:15 AM The Market for Election Equipment and Technology: What's Stopping Innovation?

Speaker:

Matthew Caulfied, University of Pennsylvania

11:35 AM Q&A with Committee

12:00 PM Lunch

12:45 PM Technology Challenges Facing Election Administrators

Speakers:

Douglas A. Kellner, State of New York
Peggy Reeves, State of Connecticut
Robert Rock, State of Rhode Island

Will Senning, State of Vermont
Anthony Stevens, State of New Hampshire

2:15 PM Q&A with Committee

3:15 PM Break

3:30 PM Rapidly Evolving Voting Technology

Speakers:

Merle King, Center for Elections Systems, Kennesaw State University
Lawrence Norden, Brennan Center for Justice at New York University

4:00 PM Q&A with Committee

4:30 PM Adjourn to Closed Session

TUESDAY, JUNE 13, 2017

OPEN SESSION

8:00 AM Continental Breakfast

8:30 AM Welcome and Introductions

Committee Co-Chairs:

Lee C. Bollinger, Columbia University
Michael A. McRobbie, Indiana University

8:45 AM Accessibility: Challenges to Access for All

Speakers:

Lisa Schur, Rutgers University
Diane Cordry Golden, Association of Assistive Technology Act Programs
Whitney Quesenbery, Center for Civic Design

9:30 AM Q&A with Committee

10:15 AM Adjourn to Closed Session

Meeting 3
Washington, DC
October 18-19, 2017

WEDNESDAY, OCTOBER 18, 2017

OPEN SESSION

8:30 AM Continental Breakfast

9:00 AM Welcome/Introductions/Meeting Overview

Committee Co-Chairs:

Lee C. Bollinger, Columbia University
Michael A. McRobbie, Indiana University

9:05 AM National Security and National Elections

Speaker:

General Michael Hayden, U.S. Air Force, National Security Agency, and Central Intelligence Agency (retired)

9:30 AM Q&A with Committee

10:10 AM Update from U.S. Department of Homeland Security on Cyber Attacks During the 2016 Election and Critical Infrastructure Policy

Speaker:

Robert Kolasky, U.S. Department of Homeland Security

10:35 AM Q&A with Committee

11:00 AM Cybersecurity Attacks: Understanding Attacks, Threats, and Policy Options

Speakers:

Matthew Blaze, University of Pennsylvania
Susan Hennessey, Brookings Institution
David Fidler, Indiana University

11:45 AM Q&A with Committee

12:15 PM Adjourn to Closed Session

OPEN SESSION

2:30 PM Election Vendors: Current Trends and a View of the Future

Speakers:

Jonathan Brill, Scytl
Jackie Harris, Democracy Live
John Schmitt, Five Cedars Group
James Simons, Everyone Counts

3:30 PM Q&A with Committee

4:00 PM Break

4:15 PM Demonstration by Election Systems Vendors

5:15 PM Adjourn to Closed Session

THURSDAY, OCTOBER 19, 2017

OPEN SESSION

8:00 AM Continental Breakfast

8:30 AM Welcome and Introductions

Committee Co-Chairs:

Lee C. Bollinger, Columbia University
Michael A. McRobbie, Indiana University

8:40 AM Overseas and Military Voting

Speaker:

David Beirne, Federal Voting Assistance Program

9:00 AM Q&A with Committee

9:30 AM Maintaining and Updating Voter Registration Databases

Speakers:

David Becker, Center for Election Innovation & Research
Shane Hamlin, Electronic Registration Information Center (ERIC)
Edgardo Cortes, State of Virginia Elections Board

10:00 AM Q&A with Committee

10:30 AM Voluntary Voting System Standard 2.0

Speaker:

Mary Brady, National Institute of Standards and Technology

10:50 AM Q&A with Committee

11:15 AM Adjourn to Closed Session

Meeting 4
Denver, CO
December 7-8, 2017

THURSDAY, DECEMBER 7, 2017

OPEN SESSION

11:00 AM Welcome/Introductions/Meeting Overview

Committee Co-Chairs:

Lee C. Bollinger, Columbia University
Michael A. McRobbie, Indiana University

11:10 AM Mail-in Ballots: The Oregon Experience

Speaker:

Brenda Bayes, State of Oregon

11:30 AM Q&A with Committee

12 noon Lunch

1:00 PM Voting: The Colorado Experience

Speakers:

Jennifer Morrell, Arapahoe County, CO
Hillary Hall, Boulder County, CO
Amber McReynolds, City and County of Denver, CO – via videoconference

1:45 PM Q&A with Committee

2:15 PM Voting: The Los Angeles County Experience

Speakers:

Kenneth Bennett, Los Angeles County, CA – via videoconference
Monica Flores, Los Angeles County, CA – via videoconference

2:30 PM Q&A with Committee

2:45 PM Break

3:00 PM Vote Centers

Speakers:

Robert M. Stein, Rice University
Joe P. Gloria, Clark County, NV

3:30 PM Q&A with Committee

4:00 PM Adjourn to Closed Session

FRIDAY, DECEMBER 8, 2017

OPEN SESSION

7:30 AM Continental Breakfast

8:00 AM Welcome and Introductions

Committee Co-Chairs:

Lee C. Bollinger, Columbia University
Michael A. McRobbie, Indiana University

8:15 AM Election Vendors: Current Trends and a View of the Future

Speakers:

Eddie Perez, Hart InterCivic
McDermot Coutts, Unisyn Voting Solutions

9:00 AM Q&A with Committee

9:30 AM Risk-limiting Audits

Speakers:

Joe Kiniry, Free & Fair – via videoconference
Neal McBurnett, Independent Election Integrity Consultant; Free & Fair
Hilary Rudy, State of Colorado

10:15 AM Q&A with Committee

10:45 AM Break

11:00 AM Education/Training/Professionalization of the Election Workforce

Speakers:

Tim Mattice, The Election Center
Kathleen Hale, Auburn University
Doug Chapin, University of Minnesota – via videoconference

11:30 AM Q&A with Committee

12:00 PM Adjourn to Closed Session

Meeting 5
Washington, DC
February 21-22, 2018

WEDNESDAY, FEBRUARY 21, 2018

OPEN SESSION

8:30 AM Continental Breakfast

9:00 AM Welcome and Introductions

Committee Co-Chairs:

Lee C. Bollinger, Columbia University
Michael A. McRobbie, Indiana University

9:05 AM	Lessons Learned from the 2016 Election: An Update

Speakers:

Connie Lawson, Secretary of State of the State of Indiana and President, National Association of Secretaries of State – via videoconference
Leslie Reynolds, Executive Director, National Association of Secretaries of State

9:30 AM	Q&A with Committee
10:00 AM	Adjourn to Closed Session

THURSDAY, FEBRUARY 22, 2018

CLOSED SESSION

Meeting 6
New York, NY
June 20, 2018

MEETING CLOSED IN ITS ENTIRETY

Appendix C

The Targeting of the American Electorate

In an assessment of Russian activities related to the 2016 presidential election, members of the the U.S. intelligence community[1] found that:

> **We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump.** We have high confidence in these judgments.[2]

The report concluded:

> **Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations.**[3]

[1] In this case, the Federal Bureau of Investigation, the Central Intelligence Agency, and the National Security Agency.

[2] Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections, Intelligence Community Assessment," January 6, 2017, p. ii, available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf. Boldface text is original to the document.

[3] Ibid.

The report also stated that the agencies "**assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton**

Social media companies later reported that, during the 2016 presidential campaign, Russian state operatives had purchased large numbers of online political ads targeting narrow segments of the American population. Facebook provided Congressional investigators with information regarding 3,000 paid ads linked to Russia.[4] Twitter identified hundreds of Russian accounts and revealed that the Russian RT news site had purchased $274,100 in online ads in 2016.[5] Google also identified Russian-bought ads aimed at influencing the 2016 election on YouTube, Gmail, and other platforms.[6]

In October 2017, Nikki Haley, U.S. Ambassador to the United Nations," stated that when a "country can . . . interfere in another country's elections, that is warfare." Misinformation creates a situation where "democracy shifts [away] from what the people want. We didn't just see it here. You can look at France, and you can look at other countries. They [Russia] are doing this everywhere. This is their new weapon of choice. And we have to make sure we get in front of it. . . . Our Intelligence agencies

and publicly contrasting her unfavorably to him. All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence;" that "Moscow's approach evolved over the course of the campaign based on Russia's understanding of the electoral prospects of the two main candidates. When it appeared to Moscow that Secretary Clinton was likely to win the election, the Russian influence campaign began to focus more on undermining her future presidency;" that "further information has come to light since Election Day that, when combined with Russian behavior since early November 2016, increases our confidence in our assessments of Russian motivations and goals;" that "**Moscow's influence campaign followed a Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries,** and paid social media users or 'trolls.' Russia, like its Soviet predecessor, has a history of conducting covert influence campaigns focused on US presidential elections that have used intelligence officers and agents and press placements to disparage candidates perceived as hostile to the Kremlin;" that "Russia's intelligence services conducted cyber operations against targets associated with the 2016 US presidential election, including targets associated with both major US political parties;" and that "We assess with high confidence that Russian military intelligence (General Staff Main Intelligence Directorate or GRU) used the Guccifer 2.0 persona and DCLeaks.com to release US victim data obtained in cyber operations publicly and in exclusives to media outlets and relayed material to WikiLeaks . . . Russia's state-run propaganda machine contributed to the influence campaign by serving as a platform for Kremlin messaging to Russian and international audiences." (See pp. ii-iii).

[4] Shane, Scott, "Facebook to Turn Over Russian-linked ads to Congress," *New York Times*, September 21, 2017.

[5] Dwoskin, Elizabeth, Adam Entous, and Karoun Demirjian, "Twitter Finds Hundreds of Accounts Tied to Russian Operatives," *Washington Post*, September 28, 2017.

[6] Dwoskin, Elizabeth, Adam Entous, and Craig Timberg "Google Uncovers Russian-Bought Ads on Youtube, Gmail and Other Platforms," *Washington Post*, October 9, 2017.

are working overtime now because there's just so much when it comes to cyber threats . . . that we are having to deal with."[7,8]

As political scientist Francis Fukuyama noted in a report to the U.S. Department of State, "the speed and scale of today's 'weaponization of information' is unprecedented . . . falsehood often travels faster than truth, leaving context and provenance behind. The traditional answer to the spread of bad information has been to inject good information . . . on the assumption that the truth would rise to the top. . . . In a world of trolls and bots, where simple facts are instantly countered by automated agents, this strategy may not be adequate. It is unclear how effectively democratic societies can continue to deliberate and function, and how hostile foreign actors can be identified and neutralized."[9]

[7] Haley, Nikki, panel with Nikki Haley, U.S. Ambassador to the United Nations and former Secretaries of State Madeleine Albright and Condoleezza Rice. The panel was part of a forum titled "The Spirit of Liberty: At Home, In the World" focused on freedom, free markets, and security and hosted by the George W. Bush Institute in New York City on October 19, 2017. Video of the panel is available at: https://www.c-span.org/video/?435568-3/ambassador-haley-secretaries-albright-rice-discuss-us-role-world&start=1885.

[8] More recently, James Clapper, former Director of National Intelligence, remarked, "As a private citizen, it's what I would call my informed opinion that, given the massive effort the Russians made, and the number of citizens that they touched, and the variety and multidimensional aspects of what they did to influence opinion . . . and given the fact that it turned on less than 80,000 votes in three states, to me it exceeds logic and credulity that they didn't affect the election. And it's my belief they actually turned it." See Sargent, Greg, "James Clapper's Bombshell: Russia Swung the Election. What If He's Right?," *Washington Post,* May 24, 2018.

[9] U.S. Advisory Commission on Public Diplomacy, *Can Public Diplomacy Survive the Internet? Bots, Echochambers, and Disinformation*, edited by Shawn Powers and Markos Kounalakis, May 2017, available at: https://www.state.gov/documents/organization/271028.pdf.

Appendix D

The Cost of Election Administration in the United States

Determining the cost of the administration of national elections is difficult. In 2001, the Caltech/MIT Voting Technology Project (VTP), in a comprehensive report about election administration in the United States, stated:

> Even the most basic facts about the cost and finance of elections in the United States are unavailable, and the most basic questions remain unexamined. It is not known how much we spend on election administration overall in the U.S. each year. It is not known on what funds are spent. There has been little analysis of how and how well local governments provide election services. Each of us has some sense of what we get—a stable and successful democracy. But there are clearly problems that can be remedied. How much will improvements in this system cost? [1]

There is general agreement that this assessment remains applicable.

The VTP conducted a survey of local elections officials in an attempt to determine the cost of conducting the 2000 presidential election. Based upon the information received from respondents, the cost was estimated to be $1 billion. The survey was repeated by the VTP in 2013 on behalf of the Presidential Commission on Election Administration, and the result was of a similar order of magnitude: around $2.6 billion.[2]

[1] Caltech/MIT Voting Technology Project, "Voting – What Is, What Could Be," 2001, p. 48, available at: http://vote.caltech.edu/reports/1.

[2] See http://web.mit.edu/supportthevoter/www/2013/12/11/pcea-public-meeting-december-3-2013-webcast-materials/.

There is little scholarly literature on the subject. The literature typically comments on the lack of comparable data, not only across states, but also often within government units across time.[3] The U.S. Census Bureau's "Census of Government" does not inquire specifically about election administration. The National Conference of State Legislatures recently reported that only four states (California, Colorado, North Dakota, and Wisconsin) collect statewide cost data.[4]

As a general matter, localities are responsible for financially supporting elections,' but how that works in practice varies across states. States typically contribute funds to support election administration. In general, states tend to be most financially and administratively responsible for voter registration systems and localities tend to have financial and administrative responsibility for staff, personnel, rent, etc. In many states, the cost of voting technology is shared between the state and localities. Some states (e.g., Rhode Island) centralize the purchase of voting technology.[5]

The federal government has played a role in the funding of elections. Federal funding for elections has been episodic and typically focused on particular projects, such as support for the purchase of new voting equipment or for security enhancements. As discussed, federal funds have been disbursed by the U.S. Election Assistance Commission (EAC). There have been discussions of an annual appropriation to states to assist with the "federal portion" of the state and local election administration, but the proposal has not gained traction.

The federal government provides support for the EAC and the National Institute of Standards and Technology (NIST). That funding is currently less than $10 million/year.[6] The federal government also provides support for the Federal Voter Assistance Program (FVAP). That funding ranges from $3.5 million to $4.0 million per year. These allocations represent the only ongoing support provided by the federal government for election administration.

[3] That literature includes Montjoy, Robert S., "The Changing Nature . . . and Costs . . . of Election Administration," *Public Administration Review*, 2010, Vol. 70, No. 6, pp. 867-875 and Hill, Sarah, "Election Administration Finance in California Counties," *The American Review of Public Administration*, 2012, Vol. 42, No. 5, pp. 606-628.

[4] See http://www.ncsl.org/research/elections-and-campaigns/the-price-of-democracy-splitting-the-bill-for-elections.aspx.

[5] For recent discussions on the topic of funding elections, see the three reports released by the National Conference of State Legislatures ("The Price of Democracy: Splitting the Bill for Elections;" "Election Costs: What States Pay;" and "Funding Elections Technology") in 2018.

[6] See https://www.eac.gov/assets/1/6/FY_2019_CBJ_Feb_12_2018_FINAL.pdf.

Appendix E

Reasons to Cast a Provisional Ballot

Reason	States
Voter eligibility cannot be immediately established—i.e., name is not on registration list	45 States + DC: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wyoming
The voter's eligibility is challenged by a poll watcher	26 States + DC: Alabama, Alaska, Arizona, Colorado, Connecticut, Delaware, District of Columbia, Florida, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Montana, Nevada, Ohio, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Utah, West Virginia, Wyoming
Voter did not present ID as required by the state	36 States + DC: Alabama, Alaska, Arizona, Arkansas, Colorado, Connecticut, District of Columbia, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Virginia, Washington, Wisconsin
Voter requested a by-mail ballot and has not cast it	16 States + DC: Alabama, Arizona, Arkansas, California, District of Columbia, Illinois, Kansas, Maryland, Montana, Nebraska, Nevada, New Jersey, Ohio, Rhode Island, Texas, Virginia, Washington

continued

Reason	States
Registration reflects an error in party listing (primary election only)	10 States + DC: California, District of Columbia, Maine, Maryland, Massachusetts, New Jersey, New York, North Carolina, Oklahoma, Pennsylvania, West Virginia
Address and/or name has changed	9 States + DC: Alaska, Arizona, California, District of Columbia, Florida, Maryland, Mississippi, New Jersey, Ohio, Texas

SOURCE: National Conference of State Legislatures, "Provisional Ballots," available at: http://www.ncsl.org/research/elections-and-campaigns/lb-provisional-ballots.aspx.

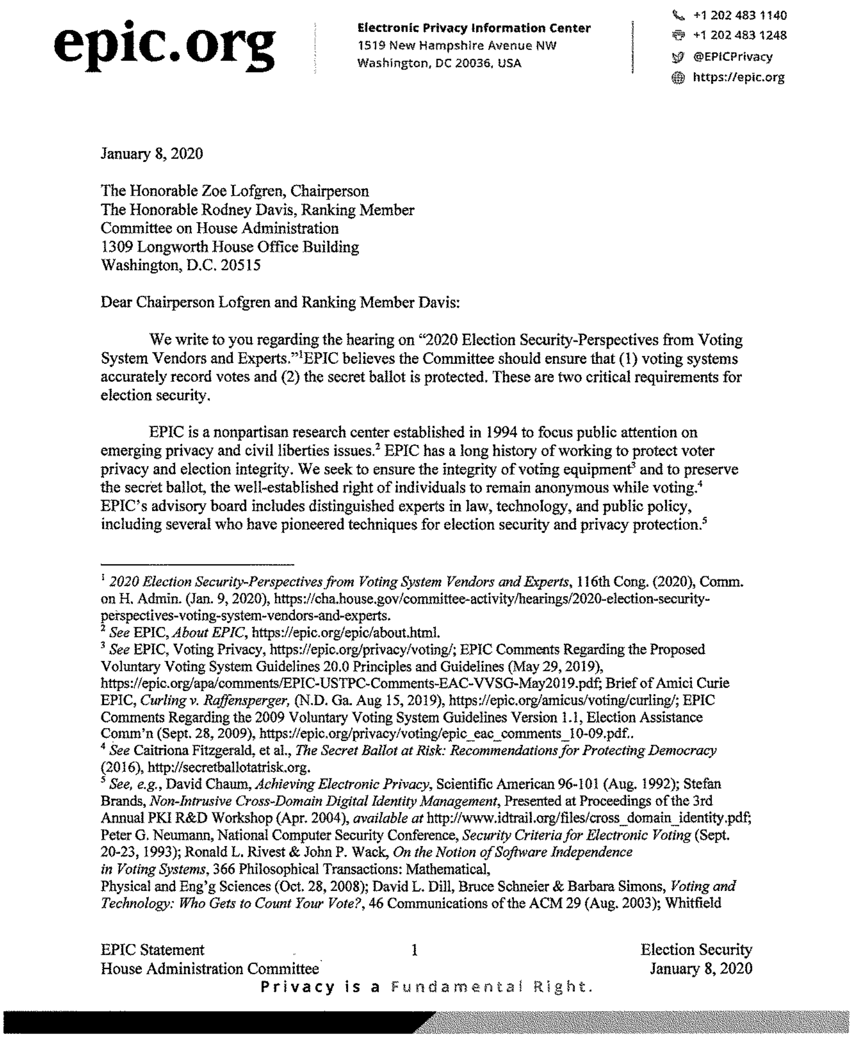
Appendix F

Acronyms and Abbreviations

ADA	Americans with Disabilities Act of 1990
ATM	Automatic teller machine
AVR	Automatic voter registration
BMD	Ballot-marking device
CAC	Common Access Card
CDF	Common Data Format
COTS	Commercial off-the-shelf
CVR	Cast vote record
DHS	U.S. Department of Homeland Security
DMV	Department of motor vehicles
DoD	U.S. Department of Defense
DoS	Denial-of-service
DRE	Direct Recording Electronic
E2E	End-to-end
E2E-V	End-to-end-verifiable
EAC	U.S. Election Assistance Commission
EAVS	Election Administration and Voting Survey
EI-ISAC	Election Infrastructure Information Sharing and Analysis Center
EPB	Electronic pollbook

ERIC	Electronic Registration Information Center
ES&S	Election Systems and Software
FEC	Federal Election Commission
FVAP	Federal Voting Assistance Program
GAO	U.S. Government Accountability Office
HAVA	Help America Vote Act of 2002
ISAC	Information Sharing and Analysis Center
IT	Information technology
MOVE	Military and Oversees Voter Empowerment Act of 2009
MPSA	Military Postal Service Agency
NAE	National Academy of Engineering
NAM	National Academy of Medicine
NAS	National Academy of Sciences
NASPAA	Network of Schools of Public Policy, Affairs, and Administration
NASS	National Association of Secretaries of State
NCLS	National Conference of State Legislatures
NIST	U.S. National Institute of Standards and Technology
NSF	U.S. National Science Foundation
NVRA	National Voter Registration Act of 1993
ODNI	Office of the Director of National Intelligence
RFP	Request for proposals
RLA	Risk-limiting audit
SSA	U.S. Social Security Administration
STAR Vote	Secure, Transparent, Auditable Reliable Vote
UOCAVA	Uniformed and Overseas Citizens Absentee Voting Act of 1986
USPS	U.S. Postal Service
VAEHA	Voting Accessibility for the Elderly and Handicapped Act of 1984
VR	Voter registration
VRA	Voting Rights Act of 1965
VRD	Voter registration database

VSAP	Voting Solutions for All People (formerly the Voting System Assessment Project)
VSTL	Voting system testing laboratories
VTP	Caltech/MIT Voting Technology Project
VVPAT	Voter-verifiable paper audit trail
VVSG	Voluntary Voting System Guidelines



epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

☎ +1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

January 8, 2020

The Honorable Zoe Lofgren, Chairperson
The Honorable Rodney Davis, Ranking Member
Committee on House Administration
1309 Longworth House Office Building
Washington, D.C. 20515

Dear Chairperson Lofgren and Ranking Member Davis:

We write to you regarding the hearing on "2020 Election Security-Perspectives from Voting System Vendors and Experts."[1]EPIC believes the Committee should ensure that (1) voting systems accurately record votes and (2) the secret ballot is protected. These are two critical requirements for election security.

EPIC is a nonpartisan research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC has a long history of working to protect voter privacy and election integrity. We seek to ensure the integrity of voting equipment[3] and to preserve the secret ballot, the well-established right of individuals to remain anonymous while voting.[4] EPIC's advisory board includes distinguished experts in law, technology, and public policy, including several who have pioneered techniques for election security and privacy protection.[5]

[1] *2020 Election Security-Perspectives from Voting System Vendors and Experts*, 116th Cong. (2020), Comm. on H. Admin. (Jan. 9, 2020), https://cha.house.gov/committee-activity/hearings/2020-election-security-perspectives-voting-system-vendors-and-experts.

[2] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.

[3] *See* EPIC, Voting Privacy, https://epic.org/privacy/voting/; EPIC Comments Regarding the Proposed Voluntary Voting System Guidelines 20.0 Principles and Guidelines (May 29, 2019), https://epic.org/apa/comments/EPIC-USTPC-Comments-EAC-VVSG-May2019.pdf; Brief of Amici Curie EPIC, *Curling v. Raffensperger,* (N.D. Ga. Aug 15, 2019), https://epic.org/amicus/voting/curling/; EPIC Comments Regarding the 2009 Voluntary Voting System Guidelines Version 1.1, Election Assistance Comm'n (Sept. 28, 2009), https://epic.org/privacy/voting/epic_eac_comments_10-09.pdf..

[4] *See* Caitriona Fitzgerald, et al., *The Secret Ballot at Risk: Recommendations for Protecting Democracy* (2016), http://secretballotatrisk.org.

[5] *See, e.g.*, David Chaum, *Achieving Electronic Privacy*, Scientific American 96-101 (Aug. 1992); Stefan Brands, *Non-Intrusive Cross-Domain Digital Identity Management*, Presented at Proceedings of the 3rd Annual PKI R&D Workshop (Apr. 2004), *available at* http://www.idtrail.org/files/cross_domain_identity.pdf; Peter G. Neumann, National Computer Security Conference, *Security Criteria for Electronic Voting* (Sept. 20-23, 1993); Ronald L. Rivest & John P. Wack, *On the Notion of Software Independence in Voting Systems*, 366 Philosophical Transactions: Mathematical, Physical and Eng'g Sciences (Oct. 28, 2008); David L. Dill, Bruce Schneier & Barbara Simons, *Voting and Technology: Who Gets to Count Your Vote?*, 46 Communications of the ACM 29 (Aug. 2003); Whitfield

Electronic voting machines are subject to manipulation, attack, and fraud. In an extensive report concerning the integrity of voting systems and the risks associated with digital technology, the National Academies of Sciences recently determined:

> [A]ll digital information—such as ballot definitions, voter choice records, vote tallies, or voter registration lists— is subject to malicious alteration; there is no technical mechanism currently available that can ensure that a computer application— such as one used to record or count votes— will produce accurate results; testing alone cannot ensure that systems have not been compromised; and any computer system used for elections— such as a voting machine or e-pollbook— can be rendered inoperable.[6]

But this is not news. For many years, computer scientists and cybersecurity experts have warned election officials that paperless balloting systems are unreliable, insecure, and unverifiable.[7] The necessary criteria for electronic voting security have long been known[8] – but the voting system vendors repeatedly fail to meet them.[9]

The drive for perfecting the election process and voting technology is grounded in a fundamental promise of our form of democracy—one vote for each person. The bar for voting technology and election administration should be set high. Voters need voting systems and procedures that reflect the best that human factors, computer science, cryptography, data protection, security, computer architecture, and informatics can produce.

We ask that this statement be entered in the hearing record. EPIC looks forward to working with the Committee on these issues of vital importance to the American public.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

Diffie, *The Evolving Meaning of Information Security*, ACM Turing award lectures (2016), https://dl.acm.org/doi/pdf/10.1145/1283920.2949031.

[6] National Academies of Sciences, Engineering, and Medicine, et al. *Securing the Vote: Protecting American Democracy* 42, 80 (National Academies Press, 2018).

[7] *See* Eric A. Fischer, Cong. Research Serv., RL32139, *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues* (2003) ("there appears to be an emerging consensus that in general, current DREs do not adhere sufficiently to currently accepted security principles for computer systems").

[8] Peter G. Neumann, National Computer Security Conference, *Security Criteria for Electronic Voting* (Sept. 20-23, 1993) (establishing the importance of reliability, accountability, and disclosability); U.S. Election Assistance Comm'n, Proposed Voluntary Voting System Guidelines 2.0 Principles and Guidelines, 84 FR 6775 (Feb. 28, 2019) (setting ballot secrecy, voter privacy, and auditability as fundamental principles), https://www.eac.gov/assets/1/6/TGDC_Recommended_VVSG2.0_P_Gs.pdf.

[9] J. Alex Halderman, Op-Ed., *I Hacked an Election. So Can the Russians*, N.Y. Times (Apr. 5, 2018).

The CHAIRPERSON. And we do thank you once again for your service here as witnesses in helping us do a better job in securing our election systems for this all-important 2020 election.

And this hearing is, without objection, now adjourned.

[Whereupon, at 12:43 p.m., the Committee was adjourned.]