

CYBERSECURITY: ENSURING THE INTEGRITY OF THE BALLOT BOX

HEARING

BEFORE THE
SUBCOMMITTEE ON
INFORMATION TECHNOLOGY
OF THE
COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES
ONE HUNDRED FOURTEENTH CONGRESS
SECOND SESSION

SEPTEMBER 28, 2016

Serial No. 114-165

Printed for the use of the Committee on Oversight and Government Reform



Available via the World Wide Web: <http://www.fdsys.gov>
<http://www.house.gov/reform>

U.S. GOVERNMENT PUBLISHING OFFICE

26-124 PDF

WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida	ELLJAH E. CUMMINGS, Maryland, <i>Ranking</i>
MICHAEL R. TURNER, Ohio	<i>Minority Member</i>
JOHN J. DUNCAN, JR., Tennessee	CAROLYN B. MALONEY, New York
JIM JORDAN, Ohio	ELEANOR HOLMES NORTON, District of
TIM WALBERG, Michigan	Columbia
JUSTIN AMASH, Michigan	WM. LACY CLAY, Missouri
PAUL A. GOSAR, Arizona	STEPHEN F. LYNCH, Massachusetts
SCOTT DESJARLAIS, Tennessee	JIM COOPER, Tennessee
TREY GOWDY, South Carolina	GERALD E. CONNOLLY, Virginia
BLAKE FARENTHOLD, Texas	TAMMY DUCKWORTH, Illinois
CYNTHIA M. LUMMIS, Wyoming	ROBIN L. KELLY, Illinois
THOMAS MASSIE, Kentucky	BRENDA L. LAWRENCE, Michigan
MARK MEADOWS, North Carolina	TED LIEU, California
RON DESANTIS, Florida	BONNIE WATSON COLEMAN, New Jersey
MICK, MULVANEY, South Carolina	STACEY E. PLASKETT, Virgin Islands
KEN BUCK, Colorado	MARK DESAULNIER, California
MARK WALKER, North Carolina	BRENDAN F. BOYLE, Pennsylvania
ROD BLUM, Iowa	PETER WELCH, Vermont
JODY B. HICE, Georgia	MICHELE LUJAN GRISHAM, New Mexico
STEVE RUSSELL, Oklahoma	
EARL L. "BUDDY" CARTER, Georgia	
GLENN GROTHMAN, Wisconsin	
WILL HURD, Texas	
GARY J. PALMER, Alabama	

JENNIFER HEMINGWAY, *Staff Director*

TROY STOCK, *Information Technology Subcommittee Staff Director*

WILLIAM MARX, *Clerk*

DAVID RAPALLO, *Minority Staff Director*

SUBCOMMITTEE ON INFORMATION TECHNOLOGY

WILL HURD, Texas, *Chairman*

BLAKE FARENTHOLD, Texas, <i>Vice Chair</i>	ROBIN L. KELLY, Illinois, <i>Ranking Minority</i>
MARK WALKER, North Carolina	<i>Member</i>
ROD BLUM, Iowa	GERALD E. CONNOLLY, Virginia
PAUL A. GOSAR, Arizona	TAMMY DUCKWORTH, Illinois
	TED LIEU, California

CONTENTS

	Page
Hearing held on September 28, 2016	1
WITNESSES	
Mr. Andy Ozment, Assistant Secretary for Cybersecurity and Communica- tions, U.S. Department of Homeland Security	
Oral Statement	5
Written Statement	8
Mr. Thomas Hicks, Commissioner, Chairman, U.S. Election Assistance Com- mission	
Oral Statement	12
Written Statement	14
The Hon. Brian P. Kemp, Secretary of State, State of Georgia	
Oral Statement	21
Written Statement	23
Mr. Andrew W. Appel, Eugene Higgins Professor of Computer Science, Prince- ton University	
Oral Statement	27
Written Statement	29
Mr. Lawrence Norden, Deputy Director, Democracy Program, Brennan Center for Justice, New York University School of Law	
Oral Statement	38
Written Statement	40
APPENDIX	
Letter for the Record regarding federal voter registration submitted by Rank- ing Member Cummings	84
Article for the Record titled, "States Ask Feds for Cybersecurity Scans Fol- lowing Election Hacking Threats," submitted by Mr. Lieu	88
Checklist for Securing Voter Registration Data, submitted by Mr. Hurd	91
Letter for the Record regarding possible Trump connections to cyber attacks, submitted by Ranking Member Cummings	93
Open letter from the National Association of Secretaries of State, submitted by Mr. Hurd	99
Statement for the Record of the Electronic Privacy Information Center, sub- mitted by Mr. Hurd	102

CYBERSECURITY: ENSURING THE INTEGRITY OF THE BALLOT BOX

Wednesday, September 28, 2016

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFORMATION TECHNOLOGY,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittee met, pursuant to call, at 2:03 p.m., in Room 2154, Rayburn House Office Building, Hon. Will Hurd [chairman of the subcommittee] presiding.

Present: Representatives Hurd, Blum, Gosar, Cummings, Kelly, Connolly, and Lieu.

Also Present: Representatives Carter and Hice.

Mr. HURD. The Subcommittee on Information Technology will come to order and, without objection, the chair is authorized to declare a recess at any time. I'd like to inform everybody, we will probably be interrupted by votes sometime between 2:30 and 3:00. So we'll get through as much of this hearing as we can and then likely reconvene after that vote series, which I think is a short series.

Thank you all for being here and good afternoon. We're here to talk about voting. Voting is the cornerstone of American democracy and a fundamental right of all Americans. Our existence as a democratic republic is only made possible and legitimate through free and fair elections. Each American's voice should be heard, but to ensure that, we must protect the ballot box. Like everything else in the digital age, however, voting can be vulnerable to hacking. There are about 10,000 election jurisdictions nationwide that administer elections, and even within States, counties use different systems and different technologies to conduct elections.

While no longer on the table for this election cycle, State and local election officials, including Secretary Kemp, who is here today, have expressed concern that classifying the election system as critical infrastructure would effectively be a Federal takeover of what has always been a local process. The purpose of this hearing is to examine the threats posed by the entities seeking to disrupt, undermine, or in any way alter the results of this election. But I also hope to initiate and foster discussion about what designating the election system as critical infrastructure would entail.

I thank the witnesses for being here today and for their efforts as fellow citizens to ensure that November's elections are free and fair.

I would like to now recognize the ranking member of the full committee, Mr. Cummings, for opening remarks.

Mr. CUMMINGS. Thank you very much, Mr. Chairman, and I thank you for your courtesy. And I thank you and Ms. Kelly for this hearing.

I want to thank all of the witnesses that are here today.

The focus today on the risk of election integrity posed by cyber threats is a very important one, but that is only a fraction of the risk to our elections. Efforts to hinder eligible voters' access to the ballot box also pose an urgent threat to our elections, to voter rights, and to our very democracy.

In January, Election Assistance Commission Executive Director Brian Newby, who I see sitting in the audience today, wrote to Alabama, Georgia and Kansas, giving the appearance that he had the unilateral authority to allow these States to change the Federal voter registration form to require proof of citizenship. Mr. Newby's invalid act led to the disenfranchisement of at least, Mr. Chairman, tens of thousands of Kansas voters alone and who knows how many more in other States.

Chairman Hicks, as the vice chairman at the time, you stated that Mr. Newby acted unilaterally and that the Commission has, quote, "affirmed that agency staff does not have the authority to make policy decisions," end of quote. I simply could not agree more. This is why I have been investigating this matter with Ranking Member Robert Brady of the Committee on House Administration, and Assistant Democratic Leader Jim Clyburn. Thankfully, a Federal Court has issued an injunction halting and reversing Mr. Newby's invalid action. However, that litigation is ongoing, and I worry about the voters who have already been turned away, perhaps never to be able to vote in this election. Chairman Hicks, Mr. Newby, Mr. Tatum, we are sending you another letter today that outlines our findings thus far.

I ask unanimous consent that the letter be entered into the record, Mr. Chairman.

Mr. HURD. Without objection, so ordered.

Mr. CUMMINGS. Thank you very much.

We learned that Mr. Newby conducted no written analysis regarding the impact of his decision on the ability of eligible voters to register to vote. He also conducted no cost-benefit analysis to compare the potential for voter fraud with the potential for eligible voter disenfranchisement. He also claimed that he had been unaware until recently that proof of citizenship laws could have a disproportionate impact on people of color. I would invite him to read the case of *John Doe v. North Carolina*. While a lengthy decision, it makes it clear that it is a major problem with regard to people of color not being able to vote.

In light of these findings, we seek additional information, but we also requested that Mr. Newby rescind his unilateral and invalid decision. Mr. Newby, I find your action to be shameful, and I hope you will swiftly rescind it.

But this is not the only threat to our right to vote. In 2013, the Supreme Court in *Shelby County v. Holder* struck down a crucial part of the Voting Rights Act that required some States to seek preclearance from the Department of Justice before changing their election laws.

Mr. Norden, your organization, the Brennan Center, has been tracking the voting restriction laws passed since Shelby. In fact, 14 States will have new voting restrictions in place this fall for the first time in a Presidential election, literally stopping American citizens from voting. These include photo ID requirements, which have been shown time and time again to unduly burden young voters, women, the elderly, people with disabilities, low-income voters, and the homeless. Passed almost exclusively by Republican legislatures, these laws have been proven to have racially discriminatory intent.

I am almost finished, Mr. Chairman.

In July, a Federal appeals court struck down the voter restrictions in North Carolina, finding that they, and I quote, listen to this, “target African Americans with almost surgical precision” and, quote, “were enacted with racially discriminatory intent in violation of the Equal Protection Clause,” end of quote.

We can fix this harmful lapse in our democracy by updating the Voting Rights Act in bills with bipartisan support and have proposed that we do so immediately. However, Republicans in Congress refuse to bring any of these bills to the floor for a vote. It is truly shameful, and as a Nation, we are better than that. I urge my colleagues to move this crucial legislation. The integrity of our democracy is at stake.

And, with that, Mr. Chairman, I thank you for your courtesy, and I yield back.

Mr. HURD. I thank the ranking member.

And now I would like to recognize the gentlelady from Illinois and my friend, Ms. Kelly, the ranking member of the Subcommittee on Information Technology, for her opening remarks.

Ms. KELLY. Thank you, Mr. Chairman.

Last week, after receiving classified briefings on threats to the upcoming election, Senator Dianne Feinstein and Representative Adam Schiff accused Russia of, and I quote, “making a serious and concerted effort to influence the U.S. election.”

Recently, Director of National Intelligence James Clapper also cited a long history of Russia’s efforts to influence elections abroad. The Director said that Russia’s apparent efforts to compromise U.S. elections, quote, “shouldn’t come as a big shock to people,” but attempts to influence the outcome of our election are not just limited to foreign government.

According to law enforcement and the FBI, cyber attacks in August against voter registration databases in my State of Illinois and Arizona were most likely criminally motivated, possibly targeting voters’ personally identifiable information. To know that my own State suffered this attack is extremely troubling, not only because of the threat of identity theft, but because of what hackers do once they have access to those databases. For example, perhaps they could change a voter’s listed party affiliation in a way that affects primary elections, or they perhaps modify voter addresses to invalidate registration. We must address these questions and do absolutely everything we can to defend against future attacks. In today’s hearing, we will be addressing the crucial question: How secure is the electoral infrastructure from any cyber attacks, regardless of the source?

According to security experts, a massive attack against the infrastructure as a whole is not the biggest cyber vulnerability in our election process. Rather, it is the individual voting machines that pose some of the greatest risk. According to a 2015 report from the Brennan Center for Justice, many voting machines were designed and engineered in the 1990s or early 2000s. These machines were designed before the Internet base of sort of advanced cyber risks that now are all too common in our current threat environment.

For example, in 2015, Virginia's Board of Elections decertified a voting system used in 24 percent of precincts after finding that an external party could access the machine's wireless feature to, quote, "record voting data or inject malicious data."

But beyond cyber attacks, these machines are also vulnerable to operational failures like crashes and glitches. As one security expert at Rice University put it, and I quote: "These machines, they barely work in a friendly environment."

As we examine this upcoming election and beyond, we must consider what sorts of investment we must make to our voting infrastructure. Today's hearing will provide us with an opportunity to learn just how vulnerable our elections might be to hackers and what our local, State, and Federal Government can do to protect our electoral processes.

But I must also add that I hope that we have more hearings on the topic of the right to vote and the access of the ballot box. Far too many States across this country have enacted troubling voter suppression laws since the Supreme Court decision in *Shelby County v. Holder*, and I have been deeply disappointed at the lack of interest across the aisle in addressing this issue. We must repair the damage done to the Voting Rights Act with legislation, and that must be a top priority. To preserve the integrity of our ballot box, we must also protect citizens' access to it.

Mr. Chairman, thank you again for holding this important hearing.

Mr. HURD. Thank you.

And I will hold the record open for 5 legislative days for any members who would like to submit a written statement.

And the chair notes the presence of our colleague Congressman Buddy Carter of Georgia. We appreciate your interest in this topic and welcome your participation today.

I ask unanimous consent that Congressman Carter be allowed to fully participate in today's hearing.

Without objection, so ordered.

We will now recognize our panel of witnesses. I am pleased to welcome Dr. Andy Ozment, Assistant Secretary for Cybersecurity and Communications at the U.S. Department of Homeland Security; Commissioner Thomas Hicks, Chairman of the U.S. Election Assistance Commission; Dr. Andrew Appel, the Eugene Higgins Professor of Computer Science at Princeton University; and Mr. Lawrence Norden, deputy director of the Democracy Program at the Brennan Center for Justice at the New York University School of Law.

I am now pleased to recognize my colleague, the gentleman from Georgia, Mr. Carter, to introduce our remaining distinguished witness.

Mr. CARTER. Well, thank you, Mr. Chairman.

It is definitely an honor today to welcome the secretary of state from the State of Georgia, my friend Brian Kemp, who preceded me in Georgia's State Senate. And I served in the house while he served in the senate, and then I moved over to the senate to try to clean up the mess that he and Tom Price left. But, nevertheless, we got that done.

Brian Kemp was elected the 27th secretary of state of Georgia in January of 2010. He has done an outstanding job in cutting wasteful spending and implementing zero-based budgeting. He currently serves as co-chair of the National Association of Secretaries of State Elections Committee and is a member of the DHS Election Infrastructure Cybersecurity Working Group. He is a native of Athens, Georgia—Go Dogs—and he and his lovely wife Marty have three beautiful daughters. And we are just glad to have him here and proud to have him representing us as our secretary of state in Georgia.

Mr. HURD. Thank you, Mr. Carter.

Welcome to you all.

And pursuant to committee rules, all witnesses will be sworn in before you testify. So please rise and raise your right hands.

Do you solemnly swear or affirm that the testimony you are about to give will be the truth, the whole truth, and nothing but the truth? Thank you and please be seated.

Let the record reflect the witnesses answered in the affirmative.

In order to allow time for discussion, please limit your testimony to 5 minutes, and your entire written statement will be made part of the record.

I would now like to recognize Dr. Ozment for his opening remarks.

WITNESS STATEMENTS

STATEMENT OF ANDY OZMENT

Mr. OZMENT. Thank you. Chairman Hurd, Ranking Member Kelly, Ranking Member Cummings, members of this committee, thank you for today's opportunity to discuss cybersecurity and our election infrastructure.

At the core of our American values is the fundamental right of all citizens to make their voice heard by having their vote counted. Ensuring the integrity of our electoral process is of vital national interest and one of our highest priorities as citizens in a democratic society. Increasingly, some parts of the Nation's election infrastructure leverage information technology for efficiency and convenience.

Like other systems, reliance on digital technologies could introduce new cybersecurity risks. However, the dispersed and diverse nature of our election infrastructure provides inherent resilience and presents real challenges to attempts at affecting the integrity of election results.

Our election system is run by State and local governments in thousands of jurisdictions across the country. Importantly, State and local officials have already been working, individually and collectively, to reduce risks and ensure the integrity of their elections.

Consistent with our longstanding work with State and local governments, we at DHS are partnering with election officials to share information about cybersecurity risks and to provide voluntary resources from the Department upon request. Addressing cybersecurity challenges such as these is not new for our Department. Our National Cybersecurity and Communications Integration Center, or NCCIC, provides support to State and local customers, such as election officials, as part of its daily operations.

In August, Secretary Johnson hosted a phone call with election officials from across the country that included representatives from other Federal agencies to discuss the cybersecurity of election infrastructure. The Secretary offered assistance from DHS' NCCIC to assist State and local election officials in securing their systems. The NCCIC provides the same assistance on an ongoing basis to public and private sector partners upon request. The assistance is voluntary and does not entail regulation, binding directives, or any kind of Federal takeover. The DHS role is limited to support only.

Through engagements with State and local officials, we are offering three types of assistance: best practices, information sharing, and incident response. In support of best practices, DHS has offered two different types of risk assessments to State and local government officials:

First, cyber hygiene scans on Internet-facing systems provide State and local officials with recurring reports that identify any vulnerabilities and provide mitigation recommendations.

Second, our cybersecurity experts can go on site to conduct risk and vulnerability assessments. These assessments are more thorough, and DHS provides the customer with a full report of vulnerabilities and recommended mitigations following the testing.

DHS will continue to share relevant information on cyber incidents through multiple avenues. For example, DHS has published best practices for securing voter registration databases and addressing potential threats to election systems. More broadly, the NCCIC works with the Multi-State Information Sharing and Analysis Center, or MS-ISAC. The MS-ISAC provides threat and vulnerability information to State and local government officials. It was created by DHS to support State, local, tribal, and territorial governments and is partially grant-funded by DHS. The MS-ISAC has a representative colocated with the NCCIC to enable regular collaboration and access to information and services for State chief information officers.

During this election season, DHS' NCCIC is prepared to provide incident response assistance to help State and local officials identify and remediate any possible cyber incidents. In the case of an attempted compromise affecting election infrastructure, the NCCIC will share technical information with other States, to assist their ability to defend their own systems from similar malicious activity.

Moving forward, we must recognize that the nature of risk facing our electoral infrastructure will continue to evolve. DHS has, therefore, established an experts group comprised of academics, independent researchers, and Federal partners. This group will continually evaluate emerging risks and ensure that State and local officials have the information and assistance needed to secure the infrastructure in their jurisdiction.

Before closing, I want to reiterate that we have confidence in the overall integrity of our electoral system, because our voting infrastructure is fundamentally resilient. It is diverse, subject to local control, and has many checks and balances built in. As the risk environment evolves, the Department will continue to support State and local partners by providing information, assistance with best practices, and tools upon request.

Thank you for the opportunity to testify, and I look forward to any questions.

[Prepared statement of Mr. Ozment follows:]



TESTIMONY

OF

DR. ANDY OZMENT
ASSISTANT SECRETARY
OFFICE OF CYBERSECURITY AND COMMUNICATIONS
NATIONAL PROTECTION AND PROGRAMS DIRECTORATE
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE
THE

HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON INFORMATION TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, D.C.

CYBERSECURITY: ENSURING THE INTEGRITY OF THE BALLOT BOX

SEPTEMBER 28, 2016

Chairman Hurd, Ranking Member Kelly, members of this Committee, thank you for the opportunity to testify. Citizens in several states and the District of Columbia have already begun voting in the 2016 general election. A majority of states and the District of Columbia allow early voting prior to November. By November 8, eligible residents of every state and territory, from every precinct, will be able to cast their votes for President, members of Congress, their local leaders, and ballot initiatives. At the core of our American values is the fundamental right of all citizens to make their voices heard by having their vote counted. Ensuring the integrity of our electoral process is a vital national interest and one of our highest priorities as citizens in a democratic society.

Our election system is funded and governed by state and local governments in thousands of jurisdictions across the country and administered by the dedicated local officials residing in those places. It is local citizens—often dedicated volunteers—who staff polling locations in their precincts and transmit the results to their election officials. Importantly, state and local officials across the country have already been working individually and collectively to reduce risks and ensure the integrity of their elections. Through existing and ongoing engagements we look forward to partnering with them to continue the work they have already started.

Increasingly, the nation's election infrastructure leverages information technology for efficiency and convenience. And like other systems, reliance on digital technologies introduces new cybersecurity risks. However, the diverse and dispersed nature of our election infrastructure provides inherent resilience and presents real challenges to a coordinated, significant incident having an impact on election results. Our National Cybersecurity and Communications Integration Center (NCCIC) helps stakeholders in federal departments and agencies, state and local governments, and the private sector to manage their cybersecurity risks. Consistent with our long-standing partnerships with state and local governments, we are working with election officials to share information about cybersecurity risks and to provide voluntary resources from the Department upon request.

Recent news reports have mentioned cyber incidents in several states this year related to election infrastructure, specifically voter registration databases. Our NCCIC has shared actionable information through direct outreach to state and local governments and through the Multi-State Information Sharing and Analysis Center (MS-ISAC), to enhance situational awareness and provide election officials with the information needed to protect themselves from similar incidents. Importantly, none of the reported incidents contain indications of malicious activity that would impact the ability of voters to cast their ballots.

Addressing cybersecurity challenges such as these is not new for our Department. At the NCCIC, we have three sets of cybersecurity customers: federal civilian agencies; state local, tribal, and territorial governments; and the private sector. The NCCIC has three lines of business to support these customers: information sharing, best practices, and incident response. Support to state and local customers, such as election officials, is part of the NCCIC's daily operations.

In August 2016, Secretary Johnson hosted a phone call with election officials from across the country that included representatives from the U.S. Election Assistance Commission, the National Institute of Standards and Technology, and the Department of Justice to discuss the

cybersecurity of election infrastructure. The Secretary offered assistance from the NCCIC to assist state and local election officials in securing their systems. The NCCIC provides this same assistance on an ongoing basis to public and private sector partners upon request. Such assistance is voluntary and does not entail regulation, binding directives, or any kind of federal “takeover,” as has been suggested by some in public discussion. No state or local election official should hesitate to request our assistance based on that misperception. DHS is only providing assistance in support of state and local authorities when they request it.

Through engagements with state and local officials, we are actively promoting a range of available services to include:

Cyber hygiene scans on Internet-facing systems. These scans are conducted remotely, after which we can provide state and local officials with a report identifying vulnerabilities and mitigation recommendations to improve the cybersecurity of systems connected to the Internet, such as online voter registration systems, election night reporting systems, and other Internet-connected election management systems. Once an agreement to provide these services is reached, DHS can complete this scan and provide the report within one week. This can be followed by weekly reports on an ongoing basis.

Risk and vulnerability assessments. These assessments are more thorough and done on-site by DHS cybersecurity experts. They typically require two to three weeks and include a wide range of vulnerability testing services, focused on both internal and external systems. When DHS conducts these assessments, we provide a full report of vulnerabilities and recommended mitigations following the testing. Given resource and time constraints, we can only conduct these assessments on a limited, first-come, first-served basis.

Incident Response Assistance. We encourage state and local election officials to report suspected malicious cyber activity to the NCCIC. On request, the NCCIC can provide on-site assistance in identifying and remediating a cyber incident. Information reported to the NCCIC is also critical to the federal government’s ability to broadly assess malicious attempts to infiltrate election systems. This technical information will also be shared with other states to assist their ability to defend their own systems from similar malicious activity.

Information sharing. DHS will continue to share relevant information on cyber incidents through multiple means. The NCCIC works with the Multi-State Information Sharing and Analysis Center (MS-ISAC) to provide threat and vulnerability information to state and local officials. The MS-ISAC was created by DHS over a decade ago and is grant funded by DHS. The MS-ISAC role is restricted to state and local government entities. It has representatives co-located with the NCCIC to enable regular collaboration and access to information and services for state chief information officers. All states are members of the MS-ISAC. Election officials can connect with their state CIO as one way to benefit from this partnership and rapidly receive information they can use to protect their systems. State election officials may also receive incident information directly from the NCCIC.

Classified information sharing. Upon request, and subject to resource constraints, DHS is able to provide classified briefings to cleared state officials as appropriate and necessary.

Sharing of best practices. DHS is publishing best practices for securing voter registration databases and addressing potential threats to election systems from ransomware.

Field-based cybersecurity advisors and protective security advisors. DHS has personnel available in the field who can provide actionable information and connect election officials to a range of tools and resources available to improve the cybersecurity preparedness of election systems and the physical site security of voting machine storage and polling places. These advisors are also available to assist with planning and incident management assistance for both cyber and physical incidents.

Physical and protective security tools, training, and resources. DHS provides advice and tools to improve the security of polling sites and other physical election infrastructure. This guidance can be found at www.dhs.gov/hometown-security. This guidance helps to train administrative and volunteer staff on identifying and reporting suspicious activities, active shooter scenarios, and what to do if they suspect an improvised explosive device. Officials can also contact a local DHS Protective Security Advisor for access to DHS resources.

Finally, DHS is working to raise the level of cybersecurity in our electoral infrastructure over the long term. To help develop this plan, DHS has established an experts group comprised of academics, independent cybersecurity researchers, and federal partners.

Before closing, I want to reiterate that we have confidence in the overall integrity of our electoral system. Our voting infrastructure is diverse, subject to local control, and has many checks and balances built in. As the threat environment evolves, the Department will continue to work with state and local partners to make essential physical and cybersecurity tools and resources available to the public and private sectors.

Thank you for the opportunity to testify, and I look forward to any questions.

Mr. HURD. Thank you, Dr. Ozment.

Mr. Hicks, you are now recognized for 5 minutes for your opening remarks.

STATEMENT OF THOMAS HICKS

Mr. HICKS. Good afternoon, Mr. Chairman, and members of the Subcommittee on Information Technology and Committee on Oversight and Government Reform.

My name is Thomas Hicks, and I am Chairman of the United States Election Assistance Commission, or EAC. The EAC is a four-member bipartisan commission. The EAC's mission is to guide, assist, and direct the effective administration of Federal elections, through funding, innovation, guidance, and information. The EAC was charged with three duties: one, develop and administer a voting machine testing and certification program; two, develop and administer a national clearinghouse for election administration information; and three, distribute HAVA grants to States to allow them to purchase new, more secure voting machines and systems.

Since our inception, the EAC has carried its charge. Forty-seven of 50 States use EAC's voluntary voting machine testing and certification program in part or in whole. We produce the most comprehensive election administration survey in the country, and we produce volumes of materials designed to help election administrators run their elections more effectively and efficiently. Among other things, these materials help the States understand and react to the current cybersecurity threats against their voting systems. State and local election officials run the elections, and we support them.

I am here today to testify on three items: First and foremost, our elections are secure. The American election administration system inherently protects our elections and its vast size and complexity. Voters should have confidence that their voices will be counted accurately when they cast them. Second, there may be headlines related to cyber attacks and data breaches, but these headlines are not representative of our voting machines. Unlike the systems in the headlines, our voting machines are not connected to the Internet. Third, the EAC works every day to help ensure the security of our elections.

First, the security that is inherent in our election system because our system is vast and complex. Since States and territories run elections, the American election administration system is actually compiled of more than 50 administrative systems. Each State has developed its own processes for conducting Federal, State and local elections. These States and territories are made up of thousands of election jurisdictions. Often, these jurisdictions operate autonomously but report to the States.

What is important to identify in today's hearing is that there is no single or uniform national election administration system that manages elections. This means that there is no national system that a hacker or bad actor can infiltrate to affect the American elections as a whole.

The complexity of our American election assistance system both deters attacks and allows election officials to ensure the integrity of the election in the event of an attack. The complexity deters po-

tential attackers from attempting to access American elections, because the number of resources that one would need to complete such an attack may be prohibitively high. There are thousands of individuals operating, often autonomously. A bad actor would have to figure out how to successfully access a significant portion of these parts. Additionally and perhaps most importantly, voting machines are not connected to the Internet. So a bad actor would have to access these systems in person. The amount of resources required to carry out this attack would be immense.

That is not to say that no one will ever try to access American elections. Recent events in Arizona and Illinois remind us that this is not true. The breaches in Arizona and Illinois exemplify another strength in our election system. Because the State administers its own elections, the breaches in these States did not compromise the system in other States. Instead of causing a national crisis, the breaches notified election officials across the country that they should be on high alert.

With this new information, election officials across the country started administrating system security checks and doublechecked in their places and procedures. The EAC took action as well. Upon learning of these attacks, we sent a security system, testing guides, and other voting machine security information to election officials. At the EAC, we have been focused on election security since our inception as an agency, and we reacted quickly, and we realize that the current events demand our help. Both our voluntary voting system guidelines and our best practices focus is on ensuring the security of our elections.

This year, we have also created a new initiative to help election administrators better administer their elections this fall. It's called Be Ready 16. Through Be Ready 16, we distributed voting training material, current information, and guides to election officials throughout the country. We also integrated topics, such as election security, into our public meetings and roundtables. We are proud of our Be Ready 16, but it is just one example of many ways we support election officials.

In conclusion, I am here to communicate one message. That message is that our elections are secure. They are secure because the American election administration system inherently protects them. There are threats to our elections, but the voters have confidence that their votes will be counted accurately and recorded accurately when they cast them.

I thank you for your time, Mr. Chairman, Ranking Member, and other members of this committee, and I look forward to your questions.

[Prepared statement of Mr. Hicks follows:]



UNITED STATES ELECTION
ASSISTANCE COMMISSION

TESTIMONY

BEFORE THE SUBCOMMITTEE
ON INFORMATION TECHNOLOGY OF
THE COMMITTEE ON OVERSIGHT
AND GOVERNMENT RELATIONS

SEPTEMBER 28, 2016

U.S. Election Assistance Commission
1335 East West Highway, Suite 4300, Silver
Spring, Maryland 20910

Introduction

Good afternoon Mr. Chairman and Members of the Subcommittee on Information Technology of the Committee on Oversight and Government Reform.

I am pleased to be here this afternoon on behalf of the U.S. Election Assistance Commission (EAC) to discuss cybersecurity and ensuring the integrity of the ballot box.

The EAC is a bipartisan commission consisting of four members; currently there are three members actively serving on the Commission. The EAC's mission is to guide, assist, and direct the effective administration of Federal elections through funding, innovation, guidance, information and regulation. The Election Assistance Commission ("the EAC") was created by the Help America Vote Act of 2002 (HAVA). HAVA was enacted after the 2000 presidential election highlighted a number of election administration concerns related to voting systems throughout the nation. The EAC was charged with three duties: (1) develop and administer a voting machine testing and certification program, (2) develop and administer a national clearing house for election administration information, and (3) distribute HAVA grants to states to allow them to purchase new, more secure voting machines and systems.

Since its inception, the EAC has and continues to carry its charge. 47 of 50 states use the EAC's voluntary voting machine Testing and Certification Program in part or as a whole; we produce the most comprehensive election administration survey in the country; and we produce volumes of materials designed to help Election Administrators run their elections more efficiently and efficaciously. These materials help the better states understand and react to the current cyber security threats against their voting systems. States and local election officials run the elections, and we support them.

Scope of My Testimony

This testimony discusses election security through three topics: (1) an overview of the American election administration system's inherent security (2) the breaches of two states' voter registration databases and how they exemplify the strength of the American election administration system, and (3) the EAC's support regarding the security of the American election administration system. Election security may only recently have been brought to many citizens' minds, but we at the EAC and election officials around the country have been focusing on the security of American elections for many years.

1. Overview of the American Election Administration System

The American election administration system is comprised of 50 states and territories. These states and territories are made up of thousands of county and local election jurisdictions. Each of these states, territories and local jurisdictions has developed their own processes and procedures for conducting federal, state and local elections. Each state's election systems are uniquely designed and autonomous from one another. There is not a single or uniform national system that manages the federal elections. Because of the decentralized nature of the American election administration system, there is no single, uniform national system that would affect the outcome of election results for the November 2016 Presidential Election. The complexity of our American election system both deters potential attacks and allows election officials to ensure the integrity of elections in the event of an attack. This complexity protects both national and state-level elections.

These many autonomous components allow states to secure their election with many layers of security. These layers start at the ballot collection process. Citizens cast their votes at a voting machine that is not connected to the internet. Physical security measures ensure that potential bad actors cannot access the voting machines without being noticed. Local election administrators collect the votes from the voting machines and physically transport, not electronically transmit, them to the election headquarters where they are tallied. This physical transportation ensures that a hacker cannot alter the tally during transportation. These results are subsequently reported to the state election official, who then reports those results to the public. States use standards of care and security procedures during this process to further ensure security. Each of these layers includes its own security processes and procedures, and each is capable of operating autonomously. These security measures are both abundant and redundant.

(a) Decentralized Election System

The American election administration system is a vast, decentralized, and non-uniform system comprised of thousands of local jurisdictions and moving parts. This decentralization establishes an inherent level of security in that it is not a uniform system with a single point of access. These attributes also allow election officials to ensure the integrity of their elections in the event of an attack by allowing election officials to monitor and audit the election process at many levels throughout the process.

First, a large amount of resources and time would be required to develop and execute an attack on the American election system because of the decentralized and non-uniform nature of the system as a whole. Because voting machines are not connected to the internet, a bad actor would need to physically access hundreds of voting machines that collect the votes. As stated above, a vast array of differing security systems and protocols protects each of these voting machines. This makes it incredibly complex to attempt to affect an election because a potential bad actor would need to learn and then access each of these systems. A bad actor would also need the man-power necessary to physically access each of these systems. Not only would a bad actor need to physically access each system, but that access would need to be done without being detected because of auditing and monitoring procedures discussed below. The resources required to complete either of these steps is immense.

To put this in perspective, consider Wisconsin, which has over one thousand four hundred (1400) local jurisdictions. Many of these jurisdictions have more than one polling place, and each of these polling places has multiple voting machines. Additionally, each one of these jurisdictions may have its own, unique security practices and protocols. So, if someone were to attempt to attack Wisconsin's elections, they would have to gain information about and successfully breach a significant portion of the voting machines in a significant portion of the 1400 jurisdictions without being detected. From a national perspective, there are more than 114,000 active polling places on Election Day. The required number of people needed to access this many different points is immense, and this surely is a deterrent against attack.

Second, the many layers of the American election system allow for monitoring and auditing of the system at each layer. The system allows election officials to be able to monitor for problems at multiple stages and incrementally verify the results of the election as not being the result of tampering.

Starting at the voting machine and progressing sequentially to the reporting of results, vote tallies and results can be and are audited in a layered, sequential format which allows for isolation and examination in the event of an error or anomaly. First, each individual voting

machine can be audited. Second, the polling location's votes can be audited as a whole. Third, the jurisdiction's results can be audited. Fourth the state's results can be audited. These many audit points are a result of the decentralized design of the system, and they also provide a method by which state election officials can detect tampering or anomalies.

It is important to note that audits are different from recounts and can identify anomalies and errors within the system. Recounts are methods by which vote tallies are verified. Recounts only ensure that votes were counted correctly. However, audits are methods by which the integrity of the system is verified. Audits ensure that the system collected votes correctly and was not compromised. As an example, some touch-screen voting machines, direct-recording electronic voting machines, store votes on memory cards, and these memory cards are used to tally votes. Many of these machines also produce a paper document that records the votes. This paper trail can then be used to verify the electronic tallies aggregated from the memory cards. This is just one of many ways voting systems are able to be audited, and auditing allows election administrators to identify and isolate attempts to tamper with the system.

The American election administration system is secure. It is secure because, by nature, it deters potential attackers with its complexity and lack of central access point. It is also secure because its design allows it to be audited; this allows election officials to isolate potential breaches, tampering, and anomalies.

2. The Recent Breaches of Voter Registration Databases in Arizona and Illinois

American Elections are secure, but this does not always prevent bad actors from attempting to affect them. This year, hackers accessed a number of computer systems related to the election, not voting systems. Breaches of these computer systems that are germane to this hearing include: (1) Arizona's voter registration list, (2) Illinois's voter registration list, and (3) the Democratic National Committee's email system. These breaches are important because they exemplify two important attributes of the American election administration system. First, while the voter registration systems were attacked, they demonstrate that the system was able to detect the hacks and the election officials were able to determine whether any data was lost or changed. Even though hackers breached the first level of security in Arizona and Illinois, the security monitoring and redundancy programs worked and election operations were not adversely affected. Second, the attacks on the voter registration databases differ in both form and potential effect from the breach of the Democratic National Convention's email system. These breaches can be used as a way to examine the security of the American election administration system and demonstrate its strength.

Based on the information we have, the breaches of the voter registration databases and the breaches of the DNC's email systems differ from each other in both form and potential effect. They differ in form because the attacks on the voter registration databases were attacks on government protected databases, while the attack on the DNC's system was on the email system. They differ in potential effect because attacks on a voter registration database do have the potential to directly affect actual election operations, i.e. interfere with voters' ability to obtain a ballot at the polling place, but attacks on a private committee's email servers affect only election political operations tangentially by interfering with the private committee's ability to advocate. It is important to remember that these two types of breaches are not commensurate and need to be examined separately.

When examining the breaches in Arizona and Illinois, it is important to remember that their security and redundancy systems worked. Using the above discussed layers of security, state and local election officials worked with state and federal law enforcement to quickly

identify the issue, evaluate potential impacts of the breaches, and ensure that the data was in the same condition as it was before the breach. In both cases there were processes in place to identify the intrusion, mitigate the damage, and audit the records to ensure accuracy. Had there been changes to data, election officials would have been able to identify those changes and use backup data, which they create on a regular basis as part of the system redundancy. Also, because America does not have one singular election administration system, an attack and breach of one state's voter registration system does not compromise the entire country. So, other states were not adversely affected by the breaches in Arizona and Illinois. Instead, other states were able to use these incidents as learning opportunities and able to take steps to ensure their systems remain secure.

This type of security preparedness and responsiveness is what helps keep American elections secure, even when they may be the target of some bad actors. This is why one of the many ways the EAC supports and furthers the security of the American election administration system is by helping states develop and share best practices.

3. EAC's Support of the American Election Administration System

The American election administration system is a complex system with many inherent security features. The EAC believes that every American's vote is important and should be safeguarded. That is why, since its inception, the EAC has incorporated both physical and cyber security of elections into its work. There are four areas which the EAC focuses its security efforts: (a) the EAC's Voluntary Voting System Guidelines; (b) testing; (c) monitoring; and (d) best practices, training, and guides.

(a) The EAC's Voluntary Voting System Guidelines

The Voluntary Voting System Guidelines (VVSG) are a comprehensive set of voting machine requirements. The EAC drafts, maintains, and monitors compliance with the VVSG. The VVSG include more than 1000 requirements including requirements for security, software, hardware, functionality, usability and accessibility. Within security, the VVSG focuses on general data security and more specifically data transmission. Within the topic of security, the VVSG focuses on general data security and more specifically data transmission.

Each state determines how to certify voting machines as acceptable for use in its elections. 47 out of 50 states have incorporated either the entirety or part of the VVSG system into their certification process. Some states require EAC certification of systems before the voting system may be used in the state. Other states use the VVSG to draft their own certification procedures. Still others require that EAC labs test voting systems before they may be used in the state.

What is truly innovative about the VVSG is the way in which they are drafted. Last year my fellow commissioners and I worked to update our drafting process. Alongside the National Institute of Standards and Technology (NIST), we created a system that leverages working groups and combines the expertise of government entities, private sector businesses, and private citizens to continually remain apprised of new innovations in the field. Cyber security is no exception. When redesigning the drafting structure in 2015, we made sure to include a security working group that represents the security community in the drafting process of all areas of the guidelines.

The security group is an active working group that provides up-to-date information on cyber security throughout the drafting process. For example, the electronic transmission of vote

tallies presents the potential for vulnerabilities in cyber security if the transmission system is not properly designed. However, electronic transmission of vote tallies is a desirable option for some election administrators because it saves time and resources. Techniques like our drafting structure allow us to stay ahead of these developments and their potential vulnerabilities. While the VVSG allow for electronic transmission of tallies, they only allow for this type of transmission if the voting system contains the proper security protocols. The VVSG allow election officials to develop their systems with new technologies while simultaneously ensuring that security is maintained. We are already working on the next set of guidelines.

(b) Testing and Certification

A critical part of our Testing and Certification Program is our voting system test laboratories. The EAC tests voting machines against VVSG requirements in EAC labs. When a machine meets the requirements, the EAC certifies the machine as conforming to the VVSG. In states that require EAC certification before a machine may be used in that state, completion of this process is a requirement that must be met before the machine may be procured by state officials. In all states, certification gives state officials confidence that the machines that are purchased are of the highest quality.

In the testing process, voting machines are tested against physical and cyber security requirements found in the VVSG. Regarding cyber security, machines are tested and assessed against requirements for: passwords, user roles, access controls, audit logs, vulnerabilities, and source code. Test laboratories also review system documentation for all aspects of the voting system being tested. This includes all functional models, settings, and user manuals. All testing information including test plans and test reports are available on our website for anyone to review.

These labs test voting systems against the requirements contained in the VVSG. Approval by one of these laboratories is required before our testing and certification program will certify a system. Before a laboratory can test a system under the EAC's program it must undergo a thorough accreditation process. In order to be accredited, the National Voluntary Laboratory Accreditation Program (NVLAP) must inspect the lab. Based on this inspection the Director of NIST must recommend the lab to the EAC. The EAC then conducts its own accreditation assessment to ensure full compliance with all EAC programmatic requirements. If the lab passes the EAC assessment, then the EAC may accredit the lab. Once a lab is approved and becomes operational, it is subjected to an audit conducted by the EAC or NIST to ensure the lab remains in compliance with the approval standards. Last year, the commissioners of the EAC accredited a new test laboratory for the first time in five years to allow for a more efficient and effective certification process.

Use of the Testing and Certification Program provides an additional level of security in the electoral system and gives state officials an additional level of confidence when making a purchasing decision or working to maintain their voting system.

(c) Monitoring

The EAC conducts a quality monitoring program for all EAC certified systems. Monitoring occurs throughout the entire election process, not just on Election Day. This monitoring includes: manufacturing facility audits; review and testing of operational machines; field anomaly reporting; investigation into reported field anomalies and dissemination of product advisories. All reports, system advisory notices and investigations are available to election officials and the public. Our monitoring program has successfully worked with state and local

election officials as well as voting system vendors to identify operational issues with EAC certified voting systems before the election, resolve these issues, test and certify the resolutions, and deploy the improved system before Election Day. To the EAC, monitoring is about ensuring quality of elections, and ensuring the quality of American elections is our highest priority.

(d) Best Practices, Training, and Guides

The EAC's work in security goes beyond voting machines. The EAC helps election officials focus on their elections by providing them with best practices and industry trends from around the country. We prepare and distribute best practices, training, and guides to election officials in an effort to arm election administrators with the best and most up-to-date information. These resources are in an easy-to-digest and actionable format.

Specifically regarding security, we prepare, maintain, and distribute Election Management Guidelines and Quick tips. To help ensure that the American election administration system is ready for contemporary threats and protected against potential vulnerabilities, we publish materials and training guides related to current events. For example, after learning about the hacks in Arizona and Illinois, we re-distributed our election security preparedness resources which includes a checklist for securing voter registration data. Regarding implementation, we continually publish and update our Managing Election Technology resources. These help election administrators to better implement election systems.

Ever aware of the broader community and our charge to act as the national clearing house of election administration information, we also host roundtables on a variety of topics related to voting system security, co-host symposiums with NIST about security and the Future of Voting, and ensure the topic of cyber security is present in our public meetings and other events. At the last EAC public meeting, we hosted a discussion of states' best practices concerning contingency planning and system security. Experts in the field, such as Secretaries of State and testing lab directors, led a robust discussion of modern and cutting edge techniques. We invite you to attend our future meetings and watch the videos of our previous meetings which you can find online.

Conclusion

The American election administration system inherently deters bad actors who may want to adversely affect the election process, and the system allows the front line of dedicated election officials to audit and monitor the system in a way that allows them to solve problems as they arise. There will always be threats to American elections. The attacks on Arizona's and Illinois's systems reminded the country of this. The EAC, however, works everyday to ensure that local officials are best prepared to prevent these threats from coming to fruition.

Voters should have confidence in the elections. I was recently in Arizona when I was approached by a gentleman who told me that he knew American elections were secure because he had worked as a poll worker. Working as a poll worker allowed the voter to see exactly how elections work and all of the security measures that are in place in every election cycle. He was confident in our elections because he had seen them for himself. Any and all Americans who might have questions or concerns about our electoral system should volunteer as poll workers or speak to their local election officials. The time commitment of volunteering is low, and you will be providing a valuable public service.

Mr. HURD. Thank you, Mr. Hicks.
Secretary Kemp, you are now recognized for 5 minutes for your opening remarks.

STATEMENT OF BRIAN P. KEMP

Mr. KEMP. Good afternoon. And I want to thank Representative Carter for that fine introduction, and thank the committee and Chairman Hurd for inviting me to discuss election security, the safeguards on our elections, and then my perspective as the top elections official in Georgia, the eighth largest State in the Union.

As Georgia's secretary of state, I currently serve as co-chair of the National Association of Secretaries of State Elections Committee. And within the last 3 weeks, I have agreed to serve on the Department of Homeland Security's elections infrastructure cyber working group organized by Secretary Jeh Johnson.

Recent events, including the hack of the DNC database as well as successful cyber attacks against voter registration databases in Arizona and Illinois, have rightfully caused great alarm among the public as well as elections officials. However, it is imperative that we as a Nation respond the correct way to these attacks. Administering elections is a great but unique responsibility. The foundation of our republic rests on the trust that Americans have in the way that we elect representatives in our government. If that trust is eroded, our enemies know that they will create fissures in the bedrock of American democracy. We cannot allow this to happen. The D.C. response to these attacks has been to take steps toward federalizing aspects of elections, election systems, and standardizing security measures. There is a better way to face these attacks and future potential threats than what has currently been proposed by DHS with designating election systems critical infrastructure.

In discussing election security, it is important to understand the difference between the components of an election. The system is comprised of campaign systems, registration and reporting systems, as well as voting systems. Campaign systems are databases not held by the States, such as databases held by national parties. Attacks on these systems don't disrupt activities in the State's jurisdictions, although they can cause harm, as recently seen by the attack on the DNC.

Registration and reporting systems are held by the States, but they do not impact the true canvass results in an election. These systems manage the voter registration rolls and report unofficial results on election night. Although these systems are more prone to attack than the voting system, because many are Web-based platforms, attacks on these systems cannot change the votes that are cast. These systems are also tested regularly, have redundancies, failsafes, and backups.

Finally, voting systems are the actual equipment used on election day. They are nonnetwork pieces of hardware that do not connect to the Internet. They are tested by vendors, by States, and by the EAC. Even before they are deployed, they are tested again by local technicians to ensure their security and accuracy.

In looking toward November, it is important for us to address the types of threats that may come against the Nation's elections. I

view these threats in three different categories: First, there are threats that undermine the confidence in the outcome of the election. This has already started among conspiracy theorists, campaigns, and members of the media. Senator Feinstein was mentioned earlier about Russia's influence. This narrative will likely continue through canvassing and beyond. Although elections officials must be cognizant of these narratives and respond to them as needed, this threat cannot create actual harm to the system or the results of the election.

Second, there are threats that disrupt elections. These threats could be cyber attacks on Web-based systems, but they more commonly occur with threats of physical violence, verbal altercations, or misinformation distributed at polling locations. In my view, this is far more likely to occur than a coordinated hacking of each individual voting unit in the United States. This type of threat is also not only more probable to occur but also would have a greater chilling effect on election participation.

The third type of threat is altering the outcome of the election. This requires an attack on the voting system itself. However, the voting system is layered with combinations of physical and technical security to address these concerns. The voting system is the most secure system in the election space. It is not networked. It's not on the Internet. And it's tested many times in many different ways as well as having overlapping physical security features to defeat cyber attacks as well as physical attacks. This threat would require far too much coordination, planning, and ability to physically manipulate thousands of machines at thousands of locations across the United States. Although it is possible, it is not probable, and there is no evidence it has ever occurred in a U.S. election.

As I stated moments ago, Secretary Johnson responded to this threat of cyber attack when he publicly began considering designating the election system critical infrastructure. This, as you can be made aware or you could suggest, caught many elections officials by surprise, and rightfully so. The suggestion from the agency, completely regarding—unfamiliar with the election space raised the level of public concern beyond what was necessary. This decision has been criticized by elections officials and cybersecurity experts alike and really addresses one of my main concerns and is why I am so glad to be here today to answer your questions as we proceed. Thank you.

[Prepared statement of Mr. Kemp follows:]



The Office of Secretary of State

Brian P. Kemp
SECRETARY OF STATE

TESTIMONY OF GEORGIA SECRETARY OF STATE BRIAN KEMP BEFORE THE HOUSE COMMITTEE ON GOVERNMENT OVERSIGHT,

INFORMATION TECHNOLOGY SUBCOMMITTEE

Will Hurd, Chairman (R-TX)

September 28, 2016

Good afternoon. I would like to thank the Committee and Chairman Hurd for inviting me to discuss election security, the safeguards on our elections, and my perspective as the top election official in Georgia, the eighth largest state in our union.

As Georgia's Secretary of State, I currently serve as co-chair of the National Association of Secretaries of State Elections Committee, and within the last three weeks, I have agreed to serve on the Department of Homeland Security's Election Infrastructure Cyber Security Working Group, organized by Secretary Jeh Johnson.

Recent events including the hack of the DNC database, as well as successful cyber-attacks against voter registration databases in Arizona and Illinois, have rightfully caused great alarm among the public as well as election officials; however, it is imperative that we as a nation respond the correct way to these attacks.

Administering elections is a great, but unique responsibility. The foundation of our Republic rests on the trust that Americans have in the way we elect representatives in our government. If that trust is eroded, our enemies know that will create fissures in the bedrock of American democracy. We cannot allow this to happen.

The D.C. response to these attacks has been to take steps towards federalizing aspects of elections, election systems, and standardizing security measures. There is a better way to face these attacks and future potential threats than what has currently been proposed by DHS with designating elections systems critical infrastructure.

POTENTIAL THREATS AND SECURITY SAFEGUARDS

In discussing election security, it is important to understand the difference between the components of the election system. This system is actually comprised of campaign systems, registration and reporting systems, as well as voting systems.

Campaign systems are databases not held by the states, such as the databases held by national parties. Attacks on these systems do not disrupt activities within the states' jurisdiction, although they can cause harm, as seen recently by the attack on the DNC.

Registration and reporting systems are held by the states, but they do not impact the true canvassed results of an election. These systems manage the voter registration rolls and report unofficial results on election night. Although these systems are more prone to attack than the voting system because many are web-based platforms, attacks on these systems cannot change votes that are cast. These systems are also tested regularly, have redundancies, fail-safes, and backups.

Finally, voting systems are the actual equipment used on Election Day. They are non-networked pieces of hardware that do not connect to the internet. They are tested by vendors, by states, and by the EAC. Even before they are deployed they are tested again by local technicians to ensure their security and accuracy.

In looking toward November, it is important for us to address the types of threats that may come against the nation's elections. I view the threats in three different categories.

First, there are threats that undermine the confidence in the outcome of the election. This has already started among conspiracy theorists, campaigns, and members of the media. Just last week Senator Dianne Feinstein of California accused Russia of "making a serious and concerted effort to influence the U.S. election." This narrative will likely continue through canvassing and beyond. Although election officials must be cognizant of these narratives and respond to them as needed, this threat cannot create actual harm to the system or the results of the election.

Second, there are threats that disrupt elections. These threats could be cyber-attacks on web-based systems, but they more commonly occur with threats of physical violence, verbal altercations, or misinformation distributed at polling locations. In my view this is far more likely to occur than a coordinated hacking of each individual voting unit in the United States. This type of threat is also not only more probable to occur, but would also have a far greater chilling effect on election participation.

The third type of threat is altering the outcome of the election. This requires an attack on the voting system itself. However, the voting system is layered with combinations of physical and technical security to address these concerns. The voting system is the most secure system in the election space. It is not networked. It is not on the internet. It is tested many times in many different ways. It has overlapping physical security features to defeat cyber-attacks and physical attacks. This threat requires far too much coordination, planning, and ability to physically manipulate thousands of machines at thousands of locations across the United States. Although it is possible, it is not probable and there is no evidence that it has ever occurred in a U.S. election.

APPROPRIATE FEDERAL GOVERNMENT RESPONSE

As I stated a moment ago, DHS Secretary Jeh Johnson responded to this threat of cyber-attack when he publicly began considering designating the election system "Critical Infrastructure." This suggestion caught many elections officials by surprise and rightfully so. The administration of elections is a state responsibility. Moreover, this suggestion came from an agency completely unfamiliar with the elections space and raised the level of public concern beyond what was necessary. This decision has been criticized by election officials and cyber-security experts alike.

DHS has yet to outline any practical benefits or make any compelling arguments on why this designation is necessary. I agree with EAC Commissioner Christy McCormick that this designation may be the first step towards creating a new federal security standard that could create legal liabilities for states. In addition, this action may open up state databases to the federal government as well as create new avenues where previously protected documents and information may become accessible to the general public, ultimately undermining the security of our elections.

I encourage the Federal government to respect the Constitutional lines our founders created, leaving the administration of elections to the states. This arrangement, as noted by the FBI as well as the White House, makes cyber-attacks and vote tampering far more difficult as election systems are decentralized among 9000 election jurisdictions. There are certainly ways for the federal government to provide assistance while working within this framework.

For instance, best practices, cyber security research, as well certain types of cyber tools provided by DHS can be useful in election preparation. Likewise, it is useful for states to receive security bulletins from federal agencies about known or potential attacks to safely guard their systems. These limited measures are useful and beneficial as they do not compel state officials, but allow them to make informed decisions about the best interest of their state.

The risks posed by foreign government hackers, cyber criminals and everyday hacktivists are not a new concept for election officials. In fact, states are always evaluating and adapting security measures to protect the integrity of our elections as part of emergency preparedness planning.

I think I speak for all state elections officials when I say we are committed to working with national security agencies and regular federal partners to solicit input on cyber threat response and risk mitigation in our elections. However, designating voting systems or any other election system as critical infrastructure would be a federal overreach, the cost of which would not equally improve the security of elections in the United States.

LOOKING TOWARDS NOVEMBER AND BEYOND

Please keep in mind that timing is critical right now. Elections are not one-day events. Ballots have been printed, and many ballots have already been mailed to voters. Early in-person voting will begin in the next couple weeks, if not days in some states.

This is an important time for elections officials to finalize preparations for November. It is not the time for inexperienced federal agencies to guess at changes that should be made. Therefore I encourage you, as policy-makers, to listen to your Secretaries of State and elections officials.

Our elections are secure, and we are working around the clock to ensure they stay that way. We are open to federal assistance, but not in designating the elections system critical infrastructure. Uncertainty, fear mongering, and empty rhetoric during this critical time can damage Americans' trust in the election process and undermine the vote we will have in November.

Elections are the cornerstone of our republic, and defending them is an honor and a duty that I and my colleagues take very seriously. We will continue working with law enforcement agencies and stakeholders to prevent attacks on our system while preparing for November and ensuring every American has a voice in electing our nation's leaders as well as the next President of the United States.

Thank you for the opportunity to provide comment.

Mr. HURD. Thank you, Secretary Kemp.

Votes have been called, and what we'll do is we'll get to Dr. Appel's, get through your opening statement, and then we will adjourn for votes and then come back and finish with Mr. Norden and the questions.

So, Dr. Appel, you are recognized for 5 minutes.

STATEMENT OF ANDREW W. APPEL

Mr. APPEL. My name is Andrew Appel. I am professor of computer science at Princeton University. In this testimony, I don't represent my employer. I am here to give my own professional opinions as a scientist but also as an American citizen who cares deeply about protecting our democracy.

My research is in software verification, computer security, technology policy and election machinery. As I will explain, I strongly recommend that, at a minimum, the Congress seek to ensure the elimination of direct-recording electronic voting machines, sometimes called touchscreen machines, immediately after this November's election and that the Congress require that all elections be subject to sensible auditing after every election to ensure that systems are functioning properly and to prove to the American people that their votes are counted as cast.

There are cybersecurity issues in all parts of our election system: before the election, voter registration databases; during the election, voting machines; after the election, vote-tabulation/canvassing/precinct-aggregation computers. In my opening statement, I will focus on voting machines. The other topics are addressed in a recent report I have coauthored entitled "10 Things Election Officials Can Do to Help Secure and Inspire Confidence in This Fall's Elections."

In the U.S., we use two kinds primarily of voting machines: optical scanners that count paper ballots and touchscreen voting machines, also called direct-recording electronic. Each voting machine is a computer running a computer program. Whether that computer counts the votes accurately or makes mistakes or cheats by shifting votes from one candidate to another depends on what software is installed in the computer.

We all use computers, and we've all had occasion to install new software. Sometimes it's an app we purchase and install on purpose. Sometimes it's a software upgrade sent by the company that made our operating system. Installing new software in a voting machine is not really much different from installing new software in any other kind of computer. Installing new software is how you hack a voting machine to cheat.

In 2009, in the courtroom of the Superior Court of New Jersey, I demonstrated how to hack a voting machine. I wrote a vote-stealing computer program that shifts votes from one candidate to another. Installing that vote-stealing program in a voting machine takes 7 minutes per machine with a screwdriver. I did this in a secure facility, and I am confident my program has not leaked out to affect real elections. But, really, the software I built was not rocket science. Any computer programmer could write the same code. Once it's installed, it could steal elections without detection for years to come. Voting machines are often delivered to polling

places several days before the election, to elementary schools, churches, firehouses. In these locations, anyone could gain access to a voting machine for 10 minutes. Between elections, the machines are routinely opened up for maintenance by county employees or private contractors. Let's assume they have the utmost integrity, but still in the U.S. we try to run our elections so that we can trust the election results without relying on any one individual.

Other computer scientists have demonstrated similar hacks on many models of machine. This is not just one glitch in one manufacturer's machine; it's the very nature of computers.

So how can we trust our elections when it's so easy to make the computers cheat? Forty States already know the answer. Vote on optical scan paper ballots. The voter fills in the bubble next to the name of their preferred candidate, then takes this paper ballot to the scanner right there in the precinct and feeds it in. That opscan voting machine has a computer in it, and we can't 100 percent prevent that computer from being hacked, but that very paper ballot marked by the voter drops into a sealed ballot box under the opscan machine. Those ballots can be recounted by hand in a way we can trust. Unfortunately, there's still about 10 States that primarily use paperless touchscreen voting computers. There's no paper ballot to recount. After the voter touches the screen, we have to rely on the computer; that is, we have to rely on whatever program is installed in the computer that day to print out the true totals when the polls close.

So what must we do? In the near term, we must not connect the voting machines to the Internet. The same goes for those computers used to prepare the electronic ballot definition files before each election that are used to program the voting machines; that is, we must not connect the voting machines, even indirectly, to the Internet. Many able and competent election administrators already follow this best practice. I hope that all 9,000 or 10,000 counties and States that run elections follow this practice and other security best practices, but it's hard to tell whether they do consistently.

These and other best practices can help protect against hacking of voting machines by people in other countries through the Internet, but they can't protect us from mistakes, software bugs, miscalibration, insider hacking, or against local criminals with access to the machines before or after elections. So what we must do as soon as possible after November is to adopt nationwide what 40 States have already done, paper ballots marked by the voter, countable by computer, but recountable by hand.

In 2000, we saw what a disastrously unreliable technology those punch-card ballots were. So, in 2002, the Congress outlawed punch-card ballots, and that was very appropriate. I strongly recommend that the Congress seek to ensure the elimination of paperless touchscreen voting machines immediately after this November's election.

[Prepared statement of Mr. Appel follows:]



Department of Computer Science
35 Olden Street
Princeton, New Jersey 08540-5233

Andrew W. Appel
Eugene Higgins Professor of Computer Science

(609) 258-4627 appel@princeton.edu

Written testimony of Andrew W. Appel

**House Subcommittee on Information Technology
hearing on “Cybersecurity: Ensuring the Integrity of the Ballot Box”
September 28, 2016**

My name is Andrew Appel. I am Professor of Computer Science at Princeton University, where I have been on the faculty for 30 years and served 6 years as Chair of the Computer Science Department. In this testimony I do not represent my employer. I’m here to give my own professional opinions as a scientist and a technologist, but also as an American citizen who cares deeply about protecting our democracy.

My research and expertise is in software verification, applied computer security, and technology policy.

As I will explain, I strongly recommend that, at a minimum, the Congress seek to ensure the elimination of “touchscreen” voting machines, immediately after this November’s election; and that it require that all elections be subject to sensible auditing after every election to ensure that systems are functioning properly and to prove to the American people that their votes are counted as cast.

Since 2003 a significant part of my research has been on the technology and security of the equipment we Americans use for elections: voting machines and election administration computers. On the topic of election machinery, I have written 5 scientific papers and 37 short articles, taught two courses at Princeton; and done expert forensic examinations and given sworn testimony in two court cases in New Jersey. In 2009 I demonstrated in open court, in the Superior Court of New Jersey, how to hack a voting machine.

There are cybersecurity issues in all parts of our election system: before the election, voter-registration databases; during the election, voting machines; after the election, vote-tabulation / canvassing / precinct-aggregation computers.

Let me start with a general principle: When we elect our government officials, sometimes we are voting for or against the very person or political party who is in office right now, running that very election! How can we trust that this person is running the election fairly? The answer is, we organize our elections so we don’t have to trust any single person or party.

That’s why, when you go to the polls in most places, there are typically two pollworkers there, often (by law) from different political parties; and there are pollwatchers, representing the parties to make sure everything is done right. That’s why recounts are done in the presence of witnesses from both parties. We run our elections transparently so the parties can watch each other, and the result is that even the losing candidate can trust that the election was run fairly.

In the U.S. we use two general kinds of voting machines: optical-scanners, and direct-recording machines (usually called “touchscreen” voting machines). In each voting machine is a computer, running a computer program. Whether that computer counts the votes accurately, makes mistakes, or cheats by shifting votes from one candidate to another, depends on what software is installed in the computer. Everyone in this room uses computers in their daily lives, and we have all had occasion to install new software. Sometimes it’s an app we purchase and install on purpose, sometimes it’s a software upgrade sent by the company that made our operating system, or word-processor program, or whatever. Installing new software in a voting machine is not really much different from installing new software in any other kind of computer.

In New Jersey I demonstrated exactly how to craft a fraudulent, vote-stealing computer program that would shift votes from one candidate to another. I did this in a secure facility and I’m confident that it has not leaked out to affect real elections, but really the software I built was not rocket science—any competent computer programmer could write the same code. Installing that vote-stealing program in a voting machine takes about 7 minutes, per machine, with a screwdriver. Once it’s installed, it could steal elections for years to come.

Voting machines in New Jersey (and many states) are delivered to polling places several days before the election—to elementary school gymnasiums, churches, firehouses. These are not secure facilities, and anyone could gain access to a voting machine for 10 minutes. Also, the machines are stored in county warehouses: Let’s assume that these county employees or private contractors have the utmost integrity, but still, in the U.S. we try to run our elections so that we can trust the election results without relying on any one individual.

I’m not the only one who’s demonstrated how to hack a voting machine. Colleagues and students and Princeton University and elsewhere have demonstrated the same principle on several different models. This is not just one glitch in one manufacturer’s machine, it’s the very nature of computers. And some voting machines can be hacked without ever touching them, by means of computer viruses transmitted on ballot cartridges.

So how can we trust our elections when it’s so easy to make the computers cheat? Forty states already know the answer: vote on optical-scan paper ballots.¹ The voter fills in the bubble next to the name of their preferred candidate, then takes this paper ballot to the scanner—right there in the precinct—and feeds it in. That opscan voting machine has a computer in it, and we can’t 100% prevent the computer from being hacked, but that very paper ballot marked by the voter drops into a sealed ballot box under the opscan machine. That’s the ballot of record, and it can be recounted by hand, in a way we can trust.

¹ Actually, in a few of these 40 states, they use “DRE with VVPAT,” touchscreen machines equipped with a ballot printer so the voter can see that the paper record of their vote matches the selections they made on the touchscreen. This technology is not as good as optical-scan paper ballots, but I consider it adequate. DRE with VVPAT stands for “Direct Recording Electronic [voting machine] with Voter-Verified Paper Audit Trail.” Overall, my count of 40 states is approximate—the reason is that many states use different equipment in different counties. If a state uses op-scans in almost all its counties, then I just count it as an op-scan state, and so on.

Paper ballots are even better protection against fraud with systematic auditing to make sure the computers aren't cheating. You don't have to recount every ballot box, just spot-check a statistical sample. There are 12 states that do this, by law; it's a good idea, and all states should do it.

It's not just malicious hacking or deliberate cheating that this protects against. Sometimes the machines are accidentally miscalibrated, or there's an unintentional software bug; these audits catch those problems too.

Even so, in most of those 12 states, the sampling methods are weak: newer auditing methods would give higher assurance that the results are accurate, *and* actually be cheaper and less labor-intensive to implement. And in many of those states, the rules are unclear for "how much discrepancy is enough to trigger a wider audit, or trigger a full recount?"

All states should pay attention to ballot chain-of-custody (who's had access to those ballot boxes between the close of the polls and an audit or recount?) and ballot accounting (how many votes were cast in each precinct? Does that match the number of ballots? -- but there's more to ballot accounting when early voting and vote centers are used).

Unfortunately, there are still about 10 states that primarily use touchscreen voting computers. There's no paper ballot to recount. After the voter touches the screen, we have to rely on the computer—that is, we have to rely on whatever program is installed in the computer that day—to print out the true totals that night when the polls close.

So what must we do? In the near term, we must remember not to connect the voting machines directly to the Internet. The reason is that almost all computer software has security vulnerabilities—software bugs that can be exploited by attackers. It takes enormous expertise and skill to run a secure computer network, and even then one cannot achieve perfect security in the face of a determined attacker. It's unrealistic to demand perfect cybersecurity from state and county election administrators.

And don't connect the election-administration computers to the Internet, either: those computers used to prepare the electronic ballot definition files before each election, that are used to program the voting machines. That is, we must not connect the voting machines even indirectly to the Internet. There are many able and competent election administrators across the country who already know this, who already follow this "best practice." I hope that all 9000 counties and states that run elections follow this practice, but of course it's hard to tell whether they all do.

This best practice can help to protect against hacking of voting machines by people in other countries through the Internet. But it can't really protect us from insider hacking, or against local criminals with access to the machines before or after elections. So what we must do as soon as possible after November is to adopt nationwide what 40 states have already done: paper ballots, marked by the voter, countable by computer if you like but recountable by hand.

In 2000 we all saw what a disastrously unreliable technology those punch-card ballots were. So in 2002 the Congress outlawed punch-card ballots, and that was very appropriate. I strongly recommend that the Congress seek to ensure the elimination of Direct-Recording Electronic, that is, “touchscreen” voting machines, immediately after this November’s election.

Other recommendations:

Now let me turn briefly to *before* the election: voter registration databases; and *after* the election, canvassing/aggregation computers.

This month the EAC distributed to State election directors these memos:

Best Practices for Continuity of Operations (Handling Destructive Malware),

by ICS-CERT, Department of Homeland Security, 1/22/2015.

Ransomware and what to do about it [and related memos],

from DHS / DOJ / HHS, etc.

Security Tip (ST16-001): Securing Voter Registration Data,

from US-CERT, Department of Homeland Security.

<https://www.us-cert.gov/ncas/tips/ST16-001>

The information in these documents is generally accurate, expert, informative, and useful. I expect it will be helpful to election administrators. In fact, those election administrators who have not been “up to speed” on these best practices will have a lot of work to do! But *all* of these manuals are generic cybersecurity-administration advice, none of it specific to elections.

Therefore, I suggest these recommendations as an election-specific supplement to the DHS’s advice:

Ten Things Election Officials Can Do to Help Secure and Inspire Confidence in This Fall’s Elections, edited by John McCarthy, Stephanie Singer, Lawrence Norden, Whitney Quesenbery, Mark Lindeman, Andrew Appel, Kim Alexander, and Joe Kiniry, September 5, 2016.

<https://electionverification.org/wp-content/uploads/2016/09/evntop109516.pdf>

We focus not on pure cybersecurity, but on how to achieve trustworthy elections even with fallible computers. I attach this document to my testimony, and here I’ll mention just one or two points.

We can’t just disconnect voter-registration computers from the Internet; there’s a legitimate role for the Internet in serving voters this way, following appropriate state laws. But on the other hand it’s very difficult to make any computer perfectly secure against hackers on the Internet. If voters are removed from the registration list by hackers, that can cause disenfranchisement. I’m particularly concerned about pollbooks. When you show up to vote, the pollworker checks your name, address, and signature in a pollbook. In those jurisdictions where the pollbooks are electronic (running on laptop or tablet computers), I’m

particularly concerned that hacks could disable these on election day, causing chaos. So election administrators must follow best practices, such as the ones cited above, to make sure they have backups and contingency plans.

When the polls close on election night, the vote totals in each voting machine—in each precinct—are transmitted to some central computer—let’s call it “county central”—where all the precincts can be added together. It’s a best practice not to do this through the Internet; in New Jersey I believe they have one Democratic pollworker and one Republican pollworker transport the electronic ballot cartridge, along with a paper printout from the voting machine signed by witnesses in the polling place, to county central. But how can we trust that the electronic ballot cartridges are not hacked, or the county central computers?

The answer is that we set up our elections so that these computers don’t need to be trusted; of course we protect them from hacking as best we can, but even if they are hacked, the citizens and candidates can be sure of the election results. We do this—already—as follows: in each precinct when the polls close, the vote totals in that precinct are announced right there, to all witnesses present: pollworkers, party pollwatchers, and citizens. That’s the law in most states, and that’s actually the practice in most states. These pollwatchers can take these numbers back to their party’s victory party, or whatever, and compare the per-precinct numbers to the table reported by the County Clerk. And they can add up all the precincts themselves, and compare with the county-central computer. I recommend that this admirable practice, already the law in most places, should be encouraged and supported by election administrators, who have nothing to hide in the way that they run our elections.

5 September, 2016

Ten Things Election Officials Can Do to Help Secure and Inspire Confidence in This Fall's Elections

Recent high-profile cyber-attacks have drawn public attention to the security of U.S. election systems. Keeping election systems reliable and safe is an evolving challenge, as it is for any computer system. Security experts recommend the following for all computer systems, from laptops to mainframe software:

- Secure systems as well as possible and make security updates regularly.
- Assume that an attacker will breach even the best security.
- Be vigilant for signs of a breach.
- Prepare contingency plans.

Election systems have additional requirements for transparency and accuracy so the public can have confidence in election outcomes.

As computer security expert Bruce Schneier has noted, "We tend to underestimate threats that haven't happened – we discount them as theoretical.... Russian attacks against our voting system have happened. And they will happen again, unless we take action."

The ten recommendations below address these concerns by providing specific steps election officials and individuals can take during the next few weeks to reduce risk and improve public confidence in the upcoming elections. Because of local laws and regulations, not every suggestion will be appropriate to every election jurisdiction.

Many state and local election officials have already taken a number of the steps outlined below, and other groups have suggested similar actions that can be taken to increase election integrity and public confidence. But much still remains to be done.

The following list is limited to actions that can be taken in the next few weeks preceding and immediately following the election. We look forward to working with election officials and others on longer-term improvements that will increase public confidence in future elections.

Members of the Election Verification Network compiled this list in response to a recent invitation from Election Assistance Commission (EAC) Chairman Thomas Hicks. For further information, please contact the Election Verification Network.

Editors (with affiliations for identification purposes only):

John McCarthy, Verified Voting Foundation

Stephanie Singer, former Chair of the Philadelphia County Board of Election

Lawrence Norden, Democracy Program, Brennan Center for Justice at NYU School of Law

Whitney Quesenbery, Center for Civic Design

Mark Lindeman, Professor of Political Science, Bard College

Andrew Appel, Professor of Computer Science, Princeton University

Kim Alexander, President and Founder, California Voter Foundation

Joe Kiniry, Galois and Free & Fair

Ten things election officials can do to help secure and inspire confidence in this fall's elections 9/5/2016

1. Document and review security fundamentals

- List all equipment, including USB drives and memory cards. Note when each piece of equipment might be connected to the Internet (even briefly), and which systems have wireless capabilities.
- Manage access controls. For each system, list everyone who can access the system, including elections staff and third-party vendor staff. Require strong passwords for all users.
- Ensure background checks are completed for both permanent and temporary staff with access to sensitive systems, and disable access when staff leave the organization.
- Limit physical access and regularly audit sensitive and critical election systems.
- Ensure that all PC and server operating systems and software have the latest security patches.
- Train all staff on fundamental security practices.

2. Test all election systems for security vulnerabilities and ability to detect attacks

- Include voter registration, ballot delivery, voting machines and election management systems.
- Document and update pre-election testing protocols and conduct pre-election testing.
- Review and document compliance with the recommendations and security checklists prepared by the US Department of Homeland Security on best practices for security, penetration testing, network scanning, how to detect and deal with potential cyber-attacks, etc.
- Review and track FBI security alerts, such as the alert "Targeting Activity Against State Board of Election Systems" recently reported in [Yahoo News](#).
- Identify resources employed to review and assess security protocols. Where feasible, ask for third-party review of those protocols (for example, county and state IT staff with security expertise).
- Excellent resources for robust pre-election testing can be found at Washburn Research.
- Contact the [Election Verification Network](#) to find credentialed volunteer experts.

3. Reduce risks created through voting systems' connections to the internet

- For those states allowing transmission of voted ballots over networks outside the control of election officials, each voter should be warned on the website and as part of the voting process: "Returning ballots by Internet, fax or email should only be used as a last resort. Voting in person or with a mailed in absentee ballot is more secure and preserves the secrecy of the ballot."
- Assume that ballots submitted over the Internet contain malware. Print them out for official tally and retention. Carefully document and authenticate any ballots returned over the Internet.
- Document and review protocols in place for confirming and verifying online registration transactions, especially changes to registrations.
- Remind staff how to detect and report unusual system malfunctions and abnormal audit results.

Ten things election officials can do to help secure and inspire confidence in this fall's elections 9/5/2016

4. Plan for electricity, telephone, computer or communications disruptions

- For each system, detail contingency procedures (in writing) in case of failure of electricity, telephone, computer or communications systems for both voting places and central facilities.
- Create paper backups for all electronic systems such as poll books, electronic ballots, etc. and create contingency distribution plans for these paper backups.
- Develop and distribute written plans for contingencies; what will you do if
 - Your voter registration database becomes corrupted?
 - Pollbooks in some locations appear to be corrupted?
 - Too many voters require provisional ballots?
 - Wait times for voting become excessive in certain locations?
 - Many electronic voting systems refuse to turn on?

5. Train election staff and poll workers how to detect and respond to problems.

- See specific recommendations for Election Day checklists, security, etc. in "[Security insights and issues for poll workers](#)" from the [Center for Civic Design](#).
- Create and promote a forum (such as a Facebook page) for poll workers to ask and answer questions about procedures.
- Review and update documentation about how to handle challenging and unexpected situations at the polls: long lines, unauthorized observers, equipment failures, inaccurate poll books, etc.

6. Provide clear guidance on reporting election security issues and other problems

- Create an online form and a toll-free hot-line number for reporting election security issues or other problems, or add this feature to existing reporting systems. Monitor online forms and hotlines frequently before, during, and after the election.
- Encourage everyone to report suspicious behavior by anyone with access to the election systems.
- Contact state agencies, [Election Assistance Commission](#), and [Department of Homeland Security](#) to plan real-time reporting to these agencies in case of unfamiliar voting system problems.
- Provide opportunities for anonymous reporting and protection from retaliation.

7. Encourage public participation and observation of all election procedures allowed by law

- Post information prominently on your website and send press releases to local reporters, community groups and political parties inviting the public to observe.
- Publicize dates, times and locations of procedures beyond what is required by law.
- Publicize a calendar of steps leading to the election (with locations if open to the public): deadlines for voter registration and absentee, military, and overseas ballot applications; ballot

Ten things election officials can do to help secure and inspire confidence in this fall's elections 9/5/2016

design and printing deadlines; pre-election testing; election training sessions; poll opening and closing; precinct and central vote counting, and all canvassing and auditing dates and sites.

- On your web site, post copies of manuals for all procedures the public is permitted to observe, and post descriptions of procedures that the public is not permitted to observe.
- Publicize the procedures for citizens or citizens' groups to obtain permission to access records, observe procedures and verify integrity.
- For each kind of ballot (such as absentee, early voting, in-precinct, provisional), document the chain of custody of the ballot from the time the blank ballot leaves the central office to the time the voted ballot is canvassed.

8. Conduct post-election audits before certification of final results

- Without voter-verified paper ballots, effective audits are impossible.
- Compare statistical samples of voting system totals to hand counts of matched paper ballot sets.
- Recruit technical experts to assist with tests and audits. Resources for finding experts, many of whom may provide pro bono services, include the [Election Verification Network](#), professional societies such as the [American Statistical Association](#), and academic institutions.
- Prominently publicize all testing and audit results.

9. Report and publicize ballot accounting and final results in detail before certification

- Create ballot accounting reports by jurisdiction, broken down by vote location (including vote centers) and ballot type (regular, provisional, absentee, etc.).
- Include the total number of ballots cast, not just results of contests.
- Reconcile number of ballots created, number voted and number returned with counts of voters.
- If counting procedures mingle ballots from different categories (for example, if ballots cast at a vote center are mingled with precinct election-day ballots), create and distribute an explanatory document to help outside observers verify that the numbers make sense.

10. Document problems and note procedures that will require additional resources to implement

- Work with the [EAC](#) and other election jurisdictions to suggest areas for future improvement.
- Note what worked well and what needs improvement to help write best practices for the future.
- Contact the [Election Verification Network](#) if you would like to work with other election experts on improving future elections.

Mr. HURD. Thank you, Dr. Appel. The committee stands in recess until immediately following votes.

[Recess.]

Mr. HURD. The Subcommittee on Information Technology will come to order.

Thank you all for the indulgence. I think we have one more opening remark, and then we'll get to the question and answer.

Mr. Norden, bring us back in. You're recognized for 5 minutes for your opening statement.

STATEMENT OF LAWRENCE NORDEN

Mr. NORDEN. Thank you, Chairman Hurd, Ranking Member Kelly, and members of the subcommittee, for inviting me to testify today. For those who don't know, the Brennan Center at NYU Law School is a think tank and public advocacy group, a nonprofit, that works on issues of democracy and justice. And I have led the Brennan Center's work on election technology and security for over a decade.

There are two points I want to convey today. The first is that real threats to our election integrity needs to be treated with the utmost seriousness. Among other things, that means that we need to distinguish between genuine threats and sensationalistic rhetoric. Second, the biggest danger, I believe, to the integrity of our election this November are attempts to undermine public confidence in the election. Specifically, as we have heard from others, attempted attacks against voting machines are highly unlikely to have widespread impact on vote totals this November. However, attacks or malfunctions that could undermine public confidence are much easier.

I want to echo what some of the other witnesses said today. It's important when we talk, when we have public discussions about election systems and security that we distinguish between the different kinds of systems that there are. Campaign email servers are obviously very different than voter registration databases, which are very different than voting machines.

On the topic of voter registration databases, Mr. Ozment and Secretary Kemp I think did a very good job talking about the kinds of steps that are being taken to make them secure. The good news is, when it comes to the integrity of our elections, there are relatively straightforward steps to ensure that any attack or hack against voter registration databases should not prevent people from voting. Most importantly, regular backups of these systems should allow us to reconstruct lists, if—and I should emphasize this has not happened anywhere as far as I know—if data is changed on those registration databases. And as far as I know, every State does this.

On the issue of voting machines, a lot of ground has already been covered about why they are different than registration databases; that voting machines should never be connected to the Internet, that we have a decentralized system with 10,000 election jurisdictions using different machines, having different rules. And I agree with all that. The one thing I would add is, that was not noted, is the vast majority of people this November will vote either on a paper ballot that is read by a scanner or will vote on a machine

that has a paper trail that they can review, and by my estimates about 80 percent of Americans will do so. And that can serve as an important deterrent and should provide voters with confidence that there is a check to ensure that their votes have been accurately recorded. These facts and others that are detailed in my testimony and that others have mentioned make it highly unlikely that there could be a successful widespread attack to change vote totals.

Having said this, I want to talk about the problem of aging equipment in the United States. I do believe that if this is not addressed, it can do real damage to voter confidence and, therefore, the integrity of our elections. And this is particularly true now when there are discussions of Russian hacks and rigged elections so much in the public discourse.

In 2015, I oversaw a yearlong study that looked at this. We found that 42 States are using voting machines that are over a decade old this November, and that's perilously close to the end of projected lifespans for these machines, particularly those designed and engineered in the 1990s. I want to be clear that that's a rather blunt tool to measure when systems need to be replaced. I'm not saying that every machine, when it reaches 10 years old or 15 years old, is suddenly going to stop working.

Before I came into this hearing today, I saw a 1965 Ford Mustang running, and it looked like it was running perfectly; and obviously the kind of maintenance and investment that is put into machinery can allow it to work much longer. And Georgia is a great example of this. They have a project with Kennesaw State where they really invest in their equipment, and they're using machines that most other jurisdictions have had to replace, because they put that investment into them.

But the interviews that we conducted with election officials in all 50 States make it clear that there are real challenges and they're growing with aging equipment. Failures of systems during voting lead to long lines and lost votes. Outdated hardware and software means that election officials struggle to find replacement parts. We talked to a number of officials who have to go to Ebay to find critical parts, like dot matrix printer ribbons, decades-old storage devices, analog modems. And more than one official described their system as essentially jerry-rigged to hold it together. And, of course, these older systems that I'm talking about did not go through the kind of more rigorous Federal certification system that we have now for security, and as Dr. Appel noted, are disproportionately paperless.

Replacing this equipment is a major issue. In 32 States, we spoke to election officials who said they wanted to replace their equipment before the next Presidential election of 2020. In 21 States, election officials told us they didn't know where they would get their money. More recently, we interviewed about 250 local election officials, and about a clear majority said they either needed to or should replace their equipment before 2020, and 80 percent of those said that they didn't know where they would get the money for that.

So I will close on that point. Thank you.

[Prepared statement of Mr. Norden follows:]

**Committee on House Oversight and Government Reform,
Subcommittee on Information Technology
United States House of Representatives**

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

September 28, 2016

“Cybersecurity: Ensuring the Integrity of the Ballot Box”

On behalf of the Brennan Center for Justice, I thank the Subcommittee on Information and Technology for holding this hearing. We appreciate the opportunity to share with you the results of our extensive studies to ensure our nation's voting systems are more secure and reliable. The Brennan Center for Justice is a nonpartisan think tank and advocacy organization that focuses on democracy and justice. We are deeply involved in the effort to ensure accurate and fair voting, improve voter registration, and to promote policies that maximize participation of eligible citizens in elections.

For the last decade, I have led the Brennan Center's extensive work on voting technology and security. In 2005, in response to growing public concern over the security of new electronic voting systems, I chaired a task force (the "Security Task Force") of the nation's leading technologists, election experts, and security professionals assembled by the Brennan Center to analyze the security and reliability of the nation's electronic voting machines.¹ In the decade since, I have authored or co-authored numerous studies on election system security, usability, cost and design.² Most recently, with my colleague Chris Famighetti, I co-authored *America's Voting Machines at Risk*, a nearly year-long study that combined data from various public documents with surveys of more than 100 specialists familiar with voting technology, including voting machine vendors, independent technology experts and election officials in all 50 states.³ The report details the security and reliability risks associated with continuing to use equipment around the country that is rapidly approaching the end of its projected lifespan.

¹ LAWRENCE NORDEN, BRENNAN CTR. FOR JUSTICE, *THE MACHINERY OF DEMOCRACY: VOTING SYSTEM SECURITY, ACCESSIBILITY, USABILITY, AND COST 46* (2006), available at https://www.brennancenter.org/sites/default/files/publications/Machinery_Democracy.pdf.

² See e.g. LAWRENCE NORDEN ET AL., BRENNAN CTR. FOR JUSTICE, *POST-ELECTION AUDITS: RESTORING TRUST IN ELECTIONS* (2007), available at http://www.brennancenter.org/sites/default/files/legacy/d/download_file_50227.pdf; LAWRENCE NORDEN, BRENNAN CTR. FOR JUSTICE, *VOTING SYSTEM FAILURES: A DATABASE SOLUTION* (2010), available at

http://www.brennancenter.org/sites/default/files/legacy/Democracy/Voting_Machine_Failures_Online.pdf;

LAWRENCE NORDEN ET AL., BRENNAN CTR. FOR JUSTICE, *BETTER BALLOTS* (2008), available at <http://www.brennancenter.org/sites/default/files/legacy/Democracy/Better%20Ballots.pdf>; LAWRENCE NORDEN ET AL., BRENNAN CTR. FOR JUSTICE, *BETTER DESIGN, BETTER ELECTIONS* (2012), available at http://www.brennancenter.org/sites/default/files/legacy/Democracy/VRE/Better_Design_Better_Elections.pdf.

³ LAWRENCE NORDEN & CHRISTOPHER FAMIGHETTI, BRENNAN CTR. FOR JUSTICE, *AMERICA'S VOTING MACHINES AT RISK 4* (2015), available at https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.

Recent high profile hacks, particularly those related to the election, have raised public fears about the integrity of our voting system. I hope to convey four points in my testimony today:

- A. Any attempt to interfere with the integrity of American elections must be treated with extreme seriousness. Among other things, this means that **it is essential to distinguish between genuine threats from sensationalistic and heated rhetoric;**
- B. The **biggest threats to the integrity** of this November's election and our democratic system are **attempts to undermine public confidence** in the reliability of that system. Attacks against the voting machines upon which Americans cast their ballots are highly unlikely to have a widespread impact. By contrast, attacks or malfunctions that can undermine public confidence are much easier;
- C. There are **important steps that election officials and the public have taken and should take to secure this November's election** against attack or malfunctions that could impact election outcomes or public confidence in those outcomes;
- D. Longer term, we must invest in our nation's election technology infrastructure and **replace the oldest machines and equipment that over time will become less reliable and less secure.** An election with integrity will ensure that all eligible citizens have the opportunity and ability to vote, and have confidence that their votes will be counted.

I. **Distinguishing genuine threats from sensationalistic rhetoric**

To address and combat potential threats to the integrity of our elections, we must honestly assess the risks and distinguish between what is probable, possible, and conceivable but highly unlikely. In recent weeks, various sources in the media and elsewhere have raised fears of widespread hacking and fraud that could change the outcome of this November's national election. These fears are generally supported by speculation and partial information.

This is harmful to our democracy, which critically depends on the confidence of the people. Hyperbolic or inaccurate rhetoric undermines the hard work election officials are doing to ensure our elections run smoothly and shifts attention away from addressing the very real problems our election system faces.

It can be especially harmful in the event of a close national election. As I will discuss below, any attempt to attack our voting systems is far more likely to sow doubt about results than it is to change a large numbers of votes. At the same time, as equipment ages, malfunctions—such as calibration problems on touch screen machines, or freezes that result in machines being taken out of service—can become more common and further compound this mistrust.⁴

⁴NORDEN & FAMIGHETTI, *supra* note 3, at 12-14.

II. Assessing the relative risks of attacks against our election system, and steps to secure them.

When voters hear of “hacks” against our election systems, many are unlikely to distinguish between campaign e-mail servers, voter registration databases and the voting machines on which they cast their votes. Not surprisingly, after hacks against the DNC e-mail server and state registration databases were revealed, many media reports immediately jumped to the question of whether our voting machines could be hacked.⁵

For this reason, it is critical to distinguish between campaign email servers and registration databases, which are connected to the internet, and voting machines, which should never be connected to the internet. For obvious reasons, it is far easier to attack a system remotely if it is connected to the internet than if it is not.⁶

A. Threats to Voter Registration Systems and Steps to Protect Them

In the last month, we learned of attempted intrusions into the Illinois and Arizona voter registration databases. It appears that in Arizona, the state detected the attempted hack before records could be accessed.⁷ In Illinois, hackers accessed personal data from several thousand voter records, but it does not appear that any voter data was changed and the full voter registration list remained unaffected.⁸

There are evident reasons to be concerned about hackers accessing voter registration databases. The first is related to accessing of personal information. Depending on how that personal information is stored, by successfully accessing a state’s registration database, hackers may be able to obtain enough information to use it for identity theft. For this reason alone, it is critical that election officials run frequent scans to monitor and alert them for potentially abnormal activity, and otherwise employ best practices to protect against hacking. The Election Assistance Commission has provided useful guidance for securing voter registration data.⁹ Both the FBI and DHS have expertise in this area, and my understanding from several election officials around

⁵See NPR Staff, *After DNC Hack Cybersecurity Experts Worry About Old Machines, Vote Tampering*, NPR, Aug. 20, 2016, <http://www.npr.org/sections/alltechconsidered/2016/08/20/490544887/after-dnc-hack-cybersecurity-experts-worry-about-old-machines-vote-tampering>.; Laurie Segall, *Just How Secure Are Electronic Voting Machines?* CNN, Aug. 9, 2016, <http://money.cnn.com/2016/08/09/technology/voting-machine-hack-election/>.; Brian Barrett, *America’s Electronic Voting Machines Are Scarily Easy Targets*, WIRED, Aug. 2, 2016, <https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election/>.

⁶ See VA. INFO. TECHNOLOGIES AGENCY, SECURITY ASSESSMENT OF WINVOTE VOTING EQUIPMENT FOR DEPARTMENT OF ELECTIONS SECURITY ASSESSMENT (2015), available at <http://www.elections.virginia.gov/WebDocs/VotingEquipReport/WINVote-final.pdf>.

⁷ Ellen Nakashima, *Russian Hackers Targeted Arizona Election System*, THE WASH. POST, Aug. 29, 2016, https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html.

⁸ Tina Sfondeles, *Hackers Accessed Personal Info from 200,000 Illinois Voters*, CHI. SUN TIMES, Aug. 29, 2016, <http://chicago.suntimes.com/politics/hackers-accessed-personal-info-from-200000-illinois-voters/>.

⁹ U.S. ELECTIONS ASSISTANCE COMMISSION, CHECKLIST FOR SECURING VOTER REGISTRATION DATA, available at http://www.eac.gov/assets/1/Documents/Checklist_Securing_VR_Data_FINAL_5.19.16.pdf.

the country is that they are working closely with both departments to ensure they are doing all they can to prevent future attacks.

A second reason for concern about hacking of voter registration databases is related to the integrity of the election itself. If a hacker were able to delete or change voter information, this could conceivably prevent someone from voting or having their vote counted, depending on the voting rules in the affected jurisdiction. The good news is that there are relatively straightforward steps that election officials can take to ensure that such attacks are thwarted or do not impact the ability of registered voters to vote.

Perhaps most importantly, election officials should create regular backups, including paper copies, of their registration databases. As long as this is done, no manipulation of computer registration databases should prevent legitimate voters from casting a ballot, or having their votes counted. Backup lists can be reconstructed and ensure that no voter is prevented from casting a ballot on Election Day.¹⁰

Voters can also help thwart attacks against voter registration databases. They should be encouraged to check their registration on-line before the registration deadline in their state, and before going to vote, and to inform election officials if their information has been changed or deleted.

B. Threats to Voting Machines

There are over 10,000 election jurisdictions in the United States.¹¹ This means in a federal election, there are essentially more than 10,000 separate elections being run, with different voting machines, ballots, rules and security measures. While there are security benefits and weaknesses associated with such a decentralized system, one clear benefit is that it is not possible to attack the nation's voting machines in one location, as might be possible with a statewide voter registration database or campaign e-mail server.¹² Similarly, because voting is not done on machines connected to the internet, remotely attacking these machines becomes difficult if not impossible.

Still, as I will discuss below, there is much more we should do to promote the security and accuracy of our voting systems. Computer scientists have demonstrated that older equipment, in particular, can be very insecure.¹³ It is also more difficult to maintain, and more likely to fail

¹⁰ For more detail on steps that jurisdictions can take to protect their registration databases see Appendix A, *Voting System Security and Reliability Risks*.

¹¹ *Election Administration and Voting Survey FAQs*, ELECTION ASSISTANCE COMMISSION, available at http://www.eac.gov/research/election_administration_and_voting_survey_faqs.aspx.

¹² See Dr. Dan S. Wallach, Testimony Before the House Committee on Space, Science & Technology Hearing 4, Sept. 13, 2016, at <https://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-114-SY-WState-DWallach-20160913.pdf>

¹³ Ben Wofford, *How to Hack an Election in 7 Minutes*, POLITICO (Aug. 5, 2016), <http://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144>; ARIEL J. FELDMAN ET AL., CTR. FOR INFO. TECH. POLICY AND DEP'T OF COMPUTER SCIENCE, PRINCETON UNIV., SECURITY ANALYSIS OF THE DIEBOLD ACCUVOTE-TS VOTING MACHINE (2006), available at https://www.usenix.org/legacy/event/evt07/tech/full_papers/feldman/feldman.pdf; DAVID WAGNER ET AL., UNIV. OF

(even without interference from an attacker) on Election Day.¹⁴ While small-scale attacks or failures of individual machines might not have a widespread impact on national vote totals, they can severely damage voter confidence, and would be particularly troubling in very close contests.

In the short run, we should do everything we can to minimize the impact of such attacks or failures.¹⁵ In the long run, we must treat our election infrastructure with the importance it deserves, with regular investments and upgrades.

1. Recent Improvements to Voting Machine Security

Before detailing how election security and reliability can be improved, it is important to understand the significant steps taken over the last several years to protect the integrity of our elections.

While recent hacks deserve our attention, the overwhelming majority of voting is not done over the internet. In recent years, voting machines that had their own wireless networks and could be accessed remotely have been taken out of service, making remote attacks much more difficult.¹⁶

Just as importantly, since the Help America Vote Act was passed in 2002, the Election Assistance Commission developed standards for federal certification of voting systems, which were passed in 2005, and updated in 2015.¹⁷ Today, 47 of 50 states rely on the Election Assistance Commission's (EAC) federal certification process when purchasing voting machines.¹⁸ This process includes much more rigorous security testing than previously existed.¹⁹

Finally, in the last few years, many jurisdictions have replaced their paperless computerized voting machines with systems that scan paper ballots filled out by voters, or produce a paper trail that can be reviewed by the voter. The Brennan Center estimates that this November, at least 80 percent of registered voters will make selections on a paper ballot, or vote on an electronic

CAL., BERKELEY, SECURITY ANALYSIS OF THE DIEBOLD ACCUBASIC INTERPRETER (2006), *available at* <http://nob.cs.ucdavis.edu/bishop/notes/2006-inter/2006-inter.pdf>.

¹⁴ NORDEN & FAMIGHETTI, *supra* note 3.

¹⁵ *Election 2016 Controversies: Voting System Security and Reliability Risks*, BRENNAN CTR. FOR JUSTICE, https://www.brennancenter.org/sites/default/files/analysis/Fact_Sheet_Voting_System_Security.pdf.

¹⁶ Jenna Portnoy, *Va. Bd. of Elections Votes to Decertify Some Voting Machine*, THE WASH. POST, Apr. 14, 2015, https://www.washingtonpost.com/local/virginia-politics/va-board-of-elections-votes-to-decertify-some-voting-machines/2015/04/14/46bce444-e2a6-11e4-81ea-0649268f729e_story.html.

¹⁷ BRYAN WHITENER, U.S. ELECTIONS ASSISTANCE COMMISSION, EAC UPDATES FEDERAL VOTING SYSTEM GUIDELINES, Mar. 31, 2015, *available at* <http://www.eac.gov/assets/1/Documents/EAC%20Updates%20Federal%20Voting%20System%20Guidelines-News-Release-FINAL-3-31-15-website.pdf>.

¹⁸ See Charles H. Romine, Ph.D., Testimony Before the United States House of Representatives Committee on Science, Space and Technology, Sept. 13, 2016, at <http://democrats.science.house.gov/sites/democrats.science.house.gov/files/documents/Romine%20Testimony.pdf>; BRIAN HANCOCK ET AL., BOWEN CTR. FOR PUBLIC AFFAIRS, INFRASTRUCTURE REQUIREMENTS FOR THE TESTING AND CERTIFICATION OF ELECTION SYSTEMS (2015), *available at* http://bowencenterforpublicaffairs.org/wp-content/uploads/2015/05/Infrastructure-Requirements-for-the-Testing-and-Certification-of-Election-Systems_FINAL.5.13.15.pdf.

¹⁹ ROMINE, *supra* note 18.

machine that produces a paper trail.²⁰ This extra “software independent” record provides another important security redundancy that should act as a deterrent to attack, and should provide voters with more confidence that their votes have been counted accurately. A public post-election audit of the voting machines can be used to confirm that the electronic record reported by the machine is correct.

All systems that include a software independent record that can be reviewed by the voter and checked against the electronic total should be fully accessible to all voters with disabilities. The good news is that there has been significant progress to make sure this is possible in new voting systems.²¹

2. Outdated Voting Machines Pose Integrity Risks

Despite these advances, there is still more work to do to ensure that all voting machines are as secure and reliable as possible. In our 2015 report, *America’s Voting Machines at Risk*, the Brennan Center found that this November, 42 states will use voting machines that are at least 10 years old.²² This is perilously close to the end of most machines’ projected lifespan, particularly machines designed and engineered in the late 1990s and early 2000s. Such machines make up the bulk of system purchased in the years following the passage of the Help America Vote Act. Using aging voting equipment increases the risk of failures and crashes — which can lead to long lines and lost votes.

The vast majority of paperless computerized voting machines were purchased at least a decade ago.²³ In November, some voters in 14 states will vote on these paperless machines.²⁴ Such machines do not produce record that can be reviewed by the voter, and allow election officials and the public to confirm electronic vote totals with a record that was produced independently of the software.

Aging voting systems also use outdated hardware and software. For this reason, replacement parts for older voting systems can be difficult, if not impossible, to find. Election officials reported to us that they struggle to find replacement parts for these systems (many of which are no longer manufactured) to keep them running. In several cases, officials have had to turn to eBay to find critical components like dot-matrix printer ribbons, decades old memory storage

²⁰ See *The Verifier—Polling Place Equipment—Current*, VERIFIED VOTER, <https://www.verifiedvoting.org/verifier/>.

²¹ *Remote Ballot Marking Systems: Secure and Accessible*, CTR. FOR CIVIC DESIGN, <http://civicdesign.org/projects/remote-ballot-marking/>; The Design Concepts, VOTING SYSTEMS ASSESSMENT PROJECT, <http://vsap.lavote.net/design-concepts-2/>.

²² NORDEN & FAMIGHETTI, *supra* note 3, at 9.

²³ In the last few years we have seen a shift away from paperless machines to PCOS systems Abby Goodnough & Christopher Drew, *Florida to Shift Voting System With Paper Trail*, N.Y. TIMES, Feb. 2, 2007, http://www.nytimes.com/2007/02/02/us/02voting.html?_r=1; *California Bans E-voting for Two Million in Four Counties*, USA TODAY NETWORK, May 1, 2004, http://usatoday30.usatoday.com/news/politics/elections/2004-05-01-e-voting_x.htm.

²⁴ Delaware, Georgia, Louisiana, New Jersey and South Carolina use paperless electronic voting machines as their primary polling place equipment statewide. In Arkansas, Indiana, Kansas, Kentucky, Mississippi, Pennsylvania, Tennessee, Texas, and Virginia, some portion of polling places use such paperless machines as the primary equipment. See *The Verifier—Polling Place Equipment—Current*, VERIFIED VOTER, <https://www.verifiedvoting.org/verifier/>.

devices, and analog modems.²⁵ Aging systems also frequently rely on unsupported software, like Windows XP and 2000, which does not receive regular security patches and is more vulnerable to the latest methods of cyberattack.²⁶

Finally, while nearly all of today's new voting machines go through a federal certification and testing program, many jurisdictions purchased voting machines before this process was in place. Older machines can have serious security flaws, including hacking vulnerabilities, which would be unacceptable by today's standards.

3. Steps Before November to Increase Security and Public Confidence

Americans should be comforted by the fact that while most of the public discussion of cybersecurity risks to our voting systems has happened only in the last few months, security experts and election officials have been in dialogue about this subject for years.²⁷ Long before there were stories in the media about Russian hacks into campaign e-mail servers or registration databases, these officials were working with federal, state and local officials to do everything possible to ensure our systems are secure and reliable. I know from personal conversations with election officials that many are in regular contact with the Department of Homeland Security, Federal Bureau of Investigation and the Election Assistance Commission about what they can do to redouble their efforts to ahead of November's election to help secure and inspire confidence in this year's election.

This year, working with election officials and others I have co-authored or edited *Voting System Security and Reliability Risks*, *Ten Things Election Officials Can Do to Help Secure and Inspire Confidence in This Fall's Elections*, and *Guidance for Election Officials with Aging Voting Equipment*.²⁸ The key steps recommended in these documents are already being taken by many election officials, including:

- Documenting and reviewing security fundamentals, including physical security and chain of custody practices;

²⁵ Telephone Interview with Mark Earley, Voting Sys. Manager, Leon Cnty., Fla. (Jan. 26, 2015); Telephone Interview with Paul Ziriak, Secretary, Okla. Board of Elections, and Pam Slater, Assistant Secretary, Okla. Board of Elections (Mar. 16, 2015); Telephone Interview with Kristin Mavromatis, Public Information Manager, Mecklenburg Cnty., N.C. (Apr. 9, 2015).

²⁶ Telephone Interview with Merle King, Exec. Dir., Ctr. for Election Sys., Kennesaw State Univ. (Feb. 5, 2015); Telephone Interview with Joe Rozell, Dir. of Elections, Oakland Cnty., Mich. (Feb. 24, 2015); Telephone Interview with Neal Kelley, Registrar of Voting, Orange Cnty., Cal. (Feb. 2, 2015); Telephone Interview with Ryan Macias, Voting Sys. Analyst, Sec. of State's Office, Cal. (Mar. 13, 2015); Telephone Interview with Joseph Mansky, Elections Manager, Ramsey Cnty., Minn. (Apr. 30, 2015); Telephone Interview with Sherry Poland, Dir. of Elections, Hamilton Cnty., Ohio (Feb. 18, 2015); Telephone Interview with Garth Fell, Elections and Recording Manager, Snohomish Cnty., Wash. (Apr. 30, 2015); E-mail from Jeremy Epstein, Senior Computer Scientist, SRI Int'l, to Lawrence Norden, Deputy Dir., Democracy Program, Brennan Ctr. for Justice (May 30, 2015, 15:21 EST) (on file with author).

²⁷ NORDEN, *supra* note 1, at 46.

²⁸ See Appendix A for *Voting System Security and Reliability Risks*, *Ten Things Election Officials Can Do to Help Secure and Inspire Confidence in This Fall's Elections*, and *Guidance for Election Officials with Aging Voting Equipment*

- Testing all election systems for security vulnerabilities and ability to detect attacks, including through robust public pre-election testing of every voting machine;
- Training election staff and poll workers how to detect and respond to problems, including long lines, unauthorized observers, equipment failures and inaccurate poll books.
- Ensuring sufficient emergency paper ballots are available at all places where Direct Recording Electronic voting machines are used.
- Conducting post-election audits to confirm that paper records match electronic results.
- Reviewing, and where necessary, improving “reconciliation policies” to guarantee that the number of signed-in voters matches ballot totals, and that machine and polling place totals match county and state totals.

Finally, voters can help secure our system as well. As with protecting the integrity of our voter registration lists (where voters have a vital role to play by checking their information and reporting any problems), voters can help ensure that any voting machine problems do not impact their or others’ ability to vote. Among other things, voters should vote early when possible to avoid potential delays caused by machine breakdowns on Election Day. And if voters experience problems while voting on machines, or if those machines fail, they should immediately report those problems to local election officials or poll workers and then call 866-OUR-VOTE, the Election Protection hotline, to report the problem.

4. Long Term Solutions: State and Federal Action for Improving Security and Reliability

Ultimately, securing our elections and inspiring confidence in the long term requires further investment in our election infrastructure. While the need for more up-to-date, accessible, secure and reliable voting equipment is clear, funders at the state and federal level seem unconcerned about our aging voting infrastructure. In our interviews for *Voting Machines at Risk*, election officials in 31 states told us they would like to purchase and deploy new voting machines before the next presidential election in 2020. However, officials from 22 of those states said they do not know where they will get the money to pay for new machines.²⁹ More recently, we surveyed over 250 local election officials about their need to replace aging equipment. While a clear majority said they hoped to replace their equipment before 2020, approximately 80% of them said they did not have the money or a plan to do so.³⁰

In too many states, legislatures have passed the buck to counties and towns. The frequent result, not surprisingly, is that counties with more resources and higher median incomes have replaced or have plans to replace antiquated equipment, while those with less resources, particularly poor or rural counties, are more left to cope with equipment that should be replaced.³¹

There are several steps we believe policymakers can take to ensure that our voting systems inspire confidence and are more secure and reliable over time:

²⁹ NORDEN & FAMIGHETTI, *supra* note 3, at 19.

³⁰ Forthcoming study from the BRENNAN CTR. FOR JUSTICE

³¹ NORDEN & FAMIGHETTI, *supra* note 3, at 19.

- **Replace older equipment, particularly paperless direct recording electronic machines.**
 - Congress and state legislatures need to allocate the funds for new, reliable, and secure voting systems.
 - Machines purchased with these funds should be *auditable* in accordance with the definition and requirements set by the Auditability Working Group convened by the National Institute of Standards and Technology (NIST) and reported to the U.S. Election Assistance Commission. Specifically, “[t]he transparency of a voting system with regards to the ability to verify that it has operated correctly in an election, and to identify the cause if it has not.”
 - The Auditability Working Group found that in order to satisfy these criteria a voting system must possess “Software Independence” or provide that an undetected change in the software cannot cause an undetectable error or change in the election outcome.³²

- **Require audits of election results, using paper ballots or voter verifiable paper records, to confirm electronic totals.** Today, only 26 states require that election officials conduct paper audits.³³ Audits of paper records are an additional check on machine malfunction, and provide public verification of vote totals.

- **Create standards for Internet Voting**
 - Currently 31 states allow military and overseas voters to cast ballots by fax, e-mail or internet portal. Alaska allows any qualified voter to request and return an absentee ballot via facsimile.³⁴
 - Most security experts argue that internet voting presents an especially serious security risk.³⁵
 - There are currently no federal standards for voting over the internet, via fax or by e-mail. Given all that’s come out about Russian involvement in hacking to influence the 2016 election, requiring new federal standards for such voting seems very important.³⁶

- **Provide grants to fund voting technology improvements to ensure more secure voting systems for decades to come.** There are at least three types of grants that could further these goals:

³² RONALD L. RIVEST & JOHN P. WACK, COMPUTER SCI. AND ARTIFICIAL INTELLIGENCE LAB. MASS. INST. OF TECH., CAMBRIDGE, MASS., ON THE NOTION OF “SOFTWARE INDEPENDENCE” IN VOTING SYSTEMS, (2006), available at <https://people.csail.mit.edu/rivest/pubs/RW06.pdf>.

³³ *Post Election Audits*, VERIFIED VOTING, <https://www.verifiedvoting.org/resources/post-election-audits/>.

³⁴ *Internet Voting*, VERIFIED VOTING, <https://www.verifiedvoting.org/resources/internet-voting/> (last visited Sept. 26, 2016).

³⁵ NORDEN & FAMIGHETTI, *supra* note 3, at 10.

³⁶ Computer Technologists’ Statement on Internet Voting, VERIFIED VOTING (2008), available at <https://www.verifiedvoting.org/wp-content/uploads/2012/09/InternetVotingStatement.pdf>.

1. Grants to pilot testing and implementation of voting systems that use non-proprietary open-source software (defined as voting system where the software license is made available under an Open Source license), as well as commercial or custom firmware and hardware could lead to more secure and reliable systems nationwide.
 - A key challenge in ensuring more secure and reliable voting systems is cost
 - Many experts agree that the widespread use of open source systems using commercial off the shelf hardware could dramatically decrease the cost of upgrading and replacing systems and parts.³⁷
 - Los Angeles County, California and Travis County, Texas are currently working to create such systems for their own voters. Grants to support the development of these programs, or start new ones, would increase the chance that this work could spread more quickly.³⁸
2. Grants to create a common data format allowing for voting-equipment device interoperability could increase reliability and security.
 - The National Institute of Standards and Technology is doing work to create a common data format for elections.
 - If NIST (or another organization) could create a common data format allowing for voting-equipment device interoperability, it could result in a huge saving on voting system costs (jurisdictions could mix and match equipment), making needed upgrades and replacements more viable.
3. Grants to the EAC or state election agencies for training to local election officials on machine security, maintenance, pre and post-election testing, development of contingency plans in event of cyber-attack or failures, and poll worker training.

III. Conclusion: Integrity, public confidence and access are inextricably linked

For far too long, the integrity of our elections has been presented as antithetical to access to the ballot box. In fact, the two are inextricably linked. As the Brennan Center argues in a recent report, *Election Integrity: A Pro-Voter Agenda*, ensuring that all American citizens who want to participate in our electoral system can vote is not only critical for free and fair elections, but also the best way to ensure integrity and confidence in our system.³⁹ This is why the Brennan Center has opposed laws that limit access and the ability of eligible voters to cast ballots, but seem to

³⁷ ROBERT F. BAUER ET. AL, THE AMERICAN VOTING EXPERIENCE: REPORT AND RECOMMENDATIONS OF THE PRESIDENTIAL COMMISSION ON ELECTION ADMINISTRATION, PRESIDENTIAL COMM'N ON ELECTION ADMINISTRATION, JANUARY, 2015, *available at* <https://www.supportthevoter.gov/files/2014/01/Amer-Voting-Exper-final-draft-01-09-14-508.pdf>

³⁸ NORDEN & FAMIGHETTI, *supra* note 3, at 22-25.

³⁹ MYRNA PEREZ, BRENNAN CTR. FOR JUSTICE, ELECTION INTEGRITY: A PRO-VOTER AGENDA (2016), *available at* <https://www.brennancenter.org/publication/election-integrity-pro-voter-agenda>.

have little actual security benefit. As detailed in a summary by the Brennan Center 14 states will have new voting restrictions in 2016.⁴⁰

Our aging equipment provides a clear example of how access and integrity are interdependent. Researchers from the Massachusetts Institute of Technology and Harvard estimate that in 2012 between 500,000 and 700,000 eligible voters did not vote because of long lines.⁴¹ The longer we wait to replace antiquated machines, the more likely this problem will get worse.

This challenge impacts access for voters, of course, but also the integrity of our elections and public confidence in them. In a highly partisan age, where conspiracy theories can flourish on social media, and risks associated with foreign and domestic hacking are real if too often sensationalized, it is critical that we take necessary steps ensure that the public can will have confidence in election results, and that malfunctions or vulnerabilities do not lead fair minded citizens to question the accuracy of election results.

The 2000 election was a traumatic event for American confidence in our electoral system. It is disturbing to imagine how much more difficult that event would have been for the country had it been preceded by months of overheated rhetoric about rigged elections and Russian hacks.

The nation made important changes to the way we vote in response to the 2000 election crisis, including replacing problematic equipment like punch card voting machines. But the changes came later than they should have; critics had been warning punch card machines should be replaced since at least the 1970s.⁴² We should not make the same mistake twice. Investment in the security and reliability of our voting systems should come *before* we experience another such crisis.

⁴⁰ *New Voting Restrictions in Place for 2016 Presidential Election*, BRENNAN CTR. FOR JUSTICE, <http://www.brennancenter.org/voting-restrictions-first-time-2016>.

⁴¹ Charles Stewart III & Stephen Ansolabehere, *Waiting in Line to Vote* 8 (Caltech/MIT Voting Tech. Project, Working Paper No. 114, 2013), available at http://vote.caltech.edu/documents/27/WP_114.pdf.

⁴² Jim Drinkard, *Holes in Punch-Card System Noted Long Ago*, USA TODAY, Mar. 7, 2001, <http://usatoday30.usatoday.com/news/politics/2001-03-07-voting.htm>.

Appendix A

Voting System Security and Reliability Risks

The last few weeks have brought renewed attention to the security and reliability of our voting systems. After credible reports last month that Russia was attempting to influence American elections by hacking into the DNC email server and other campaign files, new reports show the FBI has determined foreign hackers penetrated two state election databases.

This fact sheet describes what the risks to America's voting system security really are — and what states, localities, and voters can do to prevent successful attacks against the integrity of our elections.

The Brennan Center has studied the use of computerized voting systems for over a decade. In a comprehensive study released last year, we found the use of outdated voting equipment across the country presents serious security and reliability challenges.

The United States has made important advances in securing our voting technology in the last few years. Relatively few votes are cast over the internet or machines connected to the internet,¹ and the vast majority of ballots will be cast on systems that have a paper trail that allows election officials to independently verify software totals. This makes it highly unlikely that a cyberattack against our voting machines could have a widespread impact on the results of a national election.

Still, there is much more we should do to promote the security and accuracy of our voting systems. Computer scientists have demonstrated that older equipment, in particular, can be very insecure. It is also more difficult to maintain, and more likely to fail (even without interference from an attacker) on Election Day. While small-scale attacks or failures of individual machines might not have a widespread impact on national vote totals, they can severely damage voter confidence, and would be particularly troubling in very close contests.

Similarly, while proper safeguards can ensure attacks on voter registration databases don't prevent a legitimate voter from casting a ballot or having her vote counted, an attack on these systems could put voters' personal information at risk. Election officials must take all steps necessary to protect such information.

In the short run, we should do everything we can to minimize the impact of such attacks or failures. In the long run, we must treat our election infrastructure like other critical infrastructure, with regular investments and upgrades.

¹ Several states allow military and overseas voters to cast ballots by fax, e-mail or internet portal. Alaska allows any qualified voter to request and return an absentee ballot via facsimile.

BRENNAN CENTER FOR JUSTICE

Before detailing how election security and reliability can be improved, it is important to understand the significant steps that have been taken to protect the integrity of our elections over the last several years.

Improvements to Election Security

- Today, 47 of 50 states rely on the Election Assistance Commission's (EAC) federal certification process when purchasing voting machines. This process includes much more rigorous security testing than previously existed.
- While recent hacks deserve our attention, the overwhelming majority of voting is not done over the internet.
- In recent years, voting machines that could be accessed remotely have been taken out of service,² making widespread, remote attacks much more difficult.
- Many jurisdictions have replaced their paperless machines with systems that scan paper ballots filled out by voters, or produce a paper trail that can be reviewed by the voter.
- This November, at least 80 percent of registered voters will make selections on a paper ballot, or vote on an electronic machine that produces a paper trail.

Despite these advances, there is still more work to do to ensure that all voting machines are as secure and reliable as possible.

Outdated Voting Machines Pose Serious Reliability and Security Risks

- In November, 42 states will use voting machines that are at least 10 years old. This is perilously close to the end of most machines' expected lifespan. Using aging voting equipment increases the risk of failures and crashes — which can lead to long lines and lost votes.
- Aging voting systems use outdated hardware and software. For this reason, replacement parts for older voting systems can be difficult, if not impossible, to find. Aging systems also rely on unsupported software, like Windows XP and 2000, which does not receive regular security patches and is more vulnerable to the latest methods of cyberattack.
- While nearly all of today's voting machines go through a federal certification and testing program, many jurisdictions purchased voting machines before this process was in place. Older machines can have serious security flaws, including hacking vulnerabilities, which would be unacceptable by today's standards.
- In November, some voters in 14 states will vote on paperless electronic voting machines. These machines do not produce a paper record that can be reviewed by the voter, and allow election officials and the public to confirm electronic vote totals.³
- While the need for more up-to-date, secure and reliable voting equipment is clear, funders at the state and federal level seem unconcerned about our aging voting infrastructure. In at least 31 states, election jurisdictions will need new machines in the next five years, but officials from 22 of those states said they did not know how they would pay for them.

² For instance, in 2015 Virginia decertified a voting system after finding that an external party could access its wireless features to "record voting data or inject malicious data." That system had been eliminated in Pennsylvania in 2007 and Mississippi in 2013, and is no longer in use anywhere in the United States.

³ Delaware, Georgia, Louisiana, New Jersey and South Carolina use paperless electronic voting machines as their primary polling place equipment statewide. In Arkansas, Indiana, Kansas, Kentucky, Mississippi, Pennsylvania, Tennessee, Texas, and Virginia, some portion of polling places use such paperless machines as the primary equipment.

Short Term Solutions: Voters and Local Election Officials Can Enhance Security and Reliability

- Voters should vote early when possible, to avoid potential delays caused by machine breakdowns on Election Day.
- If voters experience problems while voting on machines, or if those machines fail, they should immediately report the problem to local officials or poll workers, and then call 866-OUR-VOTE, the Election Protection hotline, to report the problem.
- Election officials should report machine problems to the EAC so other jurisdictions using the same voting system are aware of potential issues.
- All state and local election officials should ensure the physical security of voting equipment and paper records at all stages of the process — whether in storage, in transit to polling places, or during an election — by implementing strong chain of custody procedures.
- All local election officials should conduct thorough pre-election testing on every voting machine and ensure emergency paper ballots are available at all places where electronic machines are used.
- All states should mandate thorough post-election audits to confirm that paper records match electronic results. Officials should also review and, where necessary, improve “reconciliation policies” to guarantee that the number of signed-in voters matches ballot totals, and that machine and polling place totals match county and state totals.

Long Term Solutions: State and Federal Action for Improving Security and Reliability

- Congress and state legislatures need to allocate the funds for new, reliable, and secure voting systems. Grants to fund voting technology improvements can ensure more secure voting systems for decades to come.
- Congress and state legislatures should require audits of election results, using paper ballots or voter verifiable paper records, to confirm electronic totals. Today, only 25 states require that election officials conduct paper audits.
- The next president and Congress must ensure the EAC has a full slate of commissioners and fill any vacancies in a timely manner. The work of the agency is critical to ensuring that local and state election officials have the best information to ensure our voting machines are secure and accurate.

Protecting the Integrity of Voter Registration Databases

- As long as states and local jurisdictions keep backups, including paper copies of their registration lists, no manipulation of state computer registration databases should prevent legitimate voters from casting a ballot, or having their votes counted.
- Voter registration databases can and should be programmed to run frequent, automated scans of registration activity to monitor for and alert election officials to potentially fraudulent or abnormal activity, such as a high volume of traffic or oddly timed traffic.
- Voter registration databases should be constructed to record transaction logs for all requests submitted to the site. This would allow officials to trace suspicious activity, or review activity after-the-fact for abnormal site traffic patterns.

BRENNAN CENTER FOR JUSTICE

- Websites providing online voter registration should employ best practices to protect against large-scale attacks, such as forcing an application to “time out” automatically after a certain period of inactivity, and using CAPTCHA tests.
- Voter registration databases should not contain any information other than what’s required to register, or specified information relevant to the administration of elections.
- States should publish — and enforce — a policy detailing use limitations (including user authorizations) and security safeguards to protect voters’ personal information in the data transfer process, the online or telephone interface, and the maintenance of the voter registration database.

5 September, 2016

Ten Things Election Officials Can Do to Help Secure and Inspire Confidence in This Fall's Elections

Recent high-profile cyber-attacks have drawn public attention to the security of U.S. election systems. Keeping election systems reliable and safe is an evolving challenge, as it is for any computer system. Security experts recommend the following for all computer systems, from laptops to mainframe software:

- Secure systems as well as possible and make security updates regularly.
- Assume that an attacker will breach even the best security.
- Be vigilant for signs of a breach.
- Prepare contingency plans.

Election systems have additional requirements for transparency and accuracy so the public can have confidence in election outcomes.

As computer security expert Bruce Schneier has noted, "We tend to underestimate threats that haven't happened – we discount them as theoretical.... Russian attacks against our voting system have happened. And they will happen again, unless we take action."

The ten recommendations below address these concerns by providing specific steps election officials and individuals can take during the next few weeks to reduce risk and improve public confidence in the upcoming elections. Because of local laws and regulations, not every suggestion will be appropriate to every election jurisdiction.

Many state and local election officials have already taken a number of the steps outlined below, and other groups have suggested similar actions that can be taken to increase election integrity and public confidence. But much still remains to be done.

The following list is limited to actions that can be taken in the next few weeks preceding and immediately following the election. We look forward to working with election officials and others on longer-term improvements that will increase public confidence in future elections.

Members of the Election Verification Network compiled this list in response to a recent invitation from Election Assistance Commission (EAC) Chairman Thomas Hicks. For further information, please contact the Election Verification Network.

Editors (with affiliations for identification purposes only):

John McCarthy, Verified Voting Foundation

Stephanie Singer, former Chair of the Philadelphia County Board of Election

Lawrence Norden, Democracy Program, Brennan Center for Justice at NYU School of Law

Whitney Quesenbery, Center for Civic Design

Mark Lindeman, Professor of Political Science, Bard College

Andrew Appel, Professor of Computer Science, Princeton University

Kim Alexander, President and Founder, California Voter Foundation

Ten things election officials can do to help secure and inspire confidence in this fall's elections 9/5/2016

1. Document and review security fundamentals

- List all equipment, including USB drives and memory cards. Note when each piece of equipment might be connected to the Internet (even briefly), and which systems have wireless capabilities.
- Manage access controls. For each system, list everyone who can access the system, including elections staff and third-party vendor staff. Require strong passwords for all users.
- Ensure background checks are completed for both permanent and temporary staff with access to sensitive systems, and disable access when staff leave the organization.
- Limit physical access and regularly audit sensitive and critical election systems.
- Ensure that all PC and server operating systems and software have the latest security patches.
- Train all staff on fundamental security practices.

2. Test all election systems for security vulnerabilities and ability to detect attacks

- Include voter registration, ballot delivery, voting machines and election management systems.
- Document and update pre-election testing protocols and conduct pre-election testing.
- Review and document compliance with the recommendations and security checklists prepared by the US Department of Homeland Security on best practices for security, penetration testing, network scanning, how to detect and deal with potential cyber-attacks, etc.
- Review and track FBI security alerts, such as the alert "Targeting Activity Against State Board of Election Systems" recently reported in [Yahoo News](#).
- Identify resources employed to review and assess security protocols. Where feasible, ask for third-party review of those protocols (for example, county and state IT staff with security expertise).
- Excellent resources for robust pre-election testing can be found at Washburn Research.
- Contact the [Election Verification Network](#) to find credentialed volunteer experts.

3. Reduce risks created through voting systems' connections to the internet

- For those states allowing transmission of voted ballots over networks outside the control of election officials, each voter should be warned on the website and as part of the voting process: "Returning ballots by Internet, fax or email should only be used as a last resort. Voting in person or with a mailed in absentee ballot is more secure and preserves the secrecy of the ballot."
- Assume that ballots submitted over the Internet contain malware. Print them out for official tally and retention. Carefully document and authenticate any ballots returned over the Internet.
- Document and review protocols in place for confirming and verifying online registration transactions, especially changes to registrations.
- Remind staff how to detect and report unusual system malfunctions and abnormal audit results.

Ten things election officials can do to help secure and inspire confidence in this fall's elections 9/5/2016

4. Plan for electricity, telephone, computer or communications disruptions

- For each system, detail contingency procedures (in writing) in case of failure of electricity, telephone, computer or communications systems for both voting places and central facilities.
- Create paper backups for all electronic systems such as poll books, electronic ballots, etc. and create contingency distribution plans for these paper backups.
- Develop and distribute written plans for contingencies; what will you do if
 - Your voter registration database becomes corrupted?
 - Pollbooks in some locations appear to be corrupted?
 - Too many voters require provisional ballots?
 - Wait times for voting become excessive in certain locations?
 - Many electronic voting systems refuse to turn on?

5. Train election staff and poll workers how to detect and respond to problems.

- See specific recommendations for Election Day checklists, security, etc. in "[Security insights and issues for poll workers](#)" from the [Center for Civic Design](#).
- Create and promote a forum (such as a Facebook page) for poll workers to ask and answer questions about procedures.
- Review and update documentation about how to handle challenging and unexpected situations at the polls: long lines, unauthorized observers, equipment failures, inaccurate poll books, etc.

6. Provide clear guidance on reporting election security issues and other problems

- Create an online form and a toll-free hot-line number for reporting election security issues or other problems, or add this feature to existing reporting systems. Monitor online forms and hotlines frequently before, during, and after the election.
- Encourage everyone to report suspicious behavior by anyone with access to the election systems.
- Contact state agencies, [Election Assistance Commission](#), and [Department of Homeland Security](#) to plan real-time reporting to these agencies in case of unfamiliar voting system problems.
- Provide opportunities for anonymous reporting and protection from retaliation.

7. Encourage public participation and observation of all election procedures allowed by law

- Post information prominently on your website and send press releases to local reporters, community groups and political parties inviting the public to observe.
- Publicize dates, times and locations of procedures beyond what is required by law.
- Publicize a calendar of steps leading to the election (with locations if open to the public): deadlines for voter registration and absentee, military, and overseas ballot applications; ballot

Ten things election officials can do to help secure and inspire confidence in this fall's elections 9/5/2016

design and printing deadlines; pre-election testing; election training sessions; poll opening and closing; precinct and central vote counting, and all canvassing and auditing dates and sites.

- On your web site, post copies of manuals for all procedures the public is permitted to observe, and post descriptions of procedures that the public is not permitted to observe.
- Publicize the procedures for citizens or citizens' groups to obtain permission to access records, observe procedures and verify integrity.
- For each kind of ballot (such as absentee, early voting, in-precinct, provisional), document the chain of custody of the ballot from the time the blank ballot leaves the central office to the time the voted ballot is canvassed.

8. Conduct post-election audits before certification of final results

- Without voter-verified paper ballots, effective audits are impossible.
- Compare statistical samples of voting system totals to hand counts of matched paper ballot sets.
- Recruit technical experts to assist with tests and audits. Resources for finding experts, many of whom may provide pro bono services, include the [Election Verification Network](#), professional societies such as the [American Statistical Association](#), and academic institutions.
- Prominently publicize all testing and audit results.

9. Report and publicize ballot accounting and final results in detail before certification

- Create ballot accounting reports by jurisdiction, broken down by vote location (including vote centers) and ballot type (regular, provisional, absentee, etc.).
- Include the total number of ballots cast, not just results of contests.
- Reconcile number of ballots created, number voted and number returned with counts of voters.
- If counting procedures mingle ballots from different categories (for example, if ballots cast at a vote center are mingled with precinct election-day ballots), create and distribute an explanatory document to help outside observers verify that the numbers make sense.

10. Document problems and note procedures that will require additional resources to implement

- Work with the [EAC](#) and other election jurisdictions to suggest areas for future improvement.
- Note what worked well and what needs improvement to help write best practices for the future.
- Contact the [Election Verification Network](#) if you would like to work with other election experts on improving future elections.

**BRENNAN
CENTER
FOR JUSTICE**
at New York University School of Law

For more information, contact Lawrence Norden at (lawrence.norden@nyu.edu, 646-292-8326) or Christopher Famighetti (christopher.famighetti@nyu.edu, 646-292-8387).

GUIDANCE FOR ELECTION OFFICIALS WITH AGING VOTING EQUIPMENT

Many jurisdictions around the country will be using equipment in 2016 that is rapidly approaching the end of its projected lifespan. Fortunately, there are steps election officials can take now to reduce the likelihood of problems on Election Day and beyond.

1. Review EAC Guidance on Reducing Machine Failures

The bipartisan EAC has published detailed guidelines on effective maintenance of aging equipment. Soon, they will also publish best practices for pre-election machine testing. Additionally, they offer tips for post-election audits and ballot reconciliation, which are critical in ensuring that equipment failures do not impact results.

2. Update Poll Worker Training

To prepare poll workers to respond effectively to possible Election Day problems, their training must cover common machine failures and their solutions. The Center for Civic Design for the National Science Foundation released a report noting that training should include explanation of Election Day checklists, as well as emphasis on their importance. These checklists should encompass both standard procedures and troubleshooting steps. Also important is giving poll workers hands-on practice, creating scenarios in training for them to react to, so that when the moment comes, they can act quickly and securely. Officials should consider forming teams of experienced poll workers who can act as first responders when something goes wrong in the polling place.

3. Prepare Contingency Plans

Particularly in jurisdictions that use DREs, it is critical that all polling places have enough paper ballots to use in the event of machine failures. Even in jurisdictions that use optical scan machines, plans should be laid to ensure that voters can cast votes securely, and without undue delay, if machine breakdowns occur.

4. Report Machine Problems to the EAC

Too often, election officials are not notified of machine defects or failures discovered by officials in other parts of the country – even when they use the same machines. The EAC should serve as a clearinghouse for such information, disseminating updates on emerging machine problems to officials nationwide. For this system to work better, state and county officials must promptly report to the EAC any problems they experience arising from aging voting machines.

5. Carefully Consider Equipment Purchases

The EAC has produced helpful suggestions for jurisdictions considering buying new equipment. Leasing is another option, one that the State of Maryland and some counties in Virginia have chosen. Linda Lamone, Election Director of the State of Maryland, and Edgardo Cortes, Elections Commissioner for Virginia could both speak to their experience with equipment leases.

Mr. HURD. Thank you, Mr. Norden.

And I'm going to recognize myself now for 5 minutes of questions. And my first question is actually for all five of you gentlemen, and we'll start with you, Mr. Norden, and go down the line. And first off, I appreciate you all's written testimony. I appreciate you all's oral testimony as well. We are in such an important time and, you know, there is decades' worth of experience sitting at this table looking at this important issue, and I think you give the American people some comfort.

And so my first question, I think this is a yes or no question to all of you all. On 8 November, can a cyber attack change the outcome of our national elections? Mr. Norden.

Mr. NORDEN. I'm confident that that will not be the case.

Mr. HURD. Dr. Appel?

Mr. APPEL. I think it's—

Mr. HURD. Secretary Kemp?

Mr. KEMP. No.

Mr. HURD. Mr. Hicks?

Mr. HICKS. No.

Mr. HURD. Dr. Ozment?

Mr. OZMENT. No.

Mr. HURD. Excellent.

Dr. Appel, Mr. Appel, excuse me, when you did your research in hacking the equipment, that was done in a controlled environment. Is that correct?

Mr. APPEL. It was done inside the State Police headquarters.

Mr. HURD. Was it one machine or were you able to access multiple machines?

Mr. APPEL. We had two machines per study.

Mr. HURD. Were they connected or did you have to access them each individually?

Mr. APPEL. These machines don't connect to any network.

Mr. HURD. So none of the machines connect to each other. Is that correct?

Mr. APPEL. The kind of machine that I hacked that we use in New Jersey do not connect to any network.

Mr. HURD. And they did not connect to any network, so that means they're not facing the Internet as well?

Mr. APPEL. That's right. In particular, the kinds of machines that we use in New Jersey, and the same machines are used in Louisiana, I don't know of any practical way to hack them through any kind of network. The only way I know that they can be hacked is by someone with physical access to them.

Mr. HURD. So there's no practical way to hack these voting machines unless you have physical access. And then if you have physical access, you have to have physical access to each box because none of the boxes are actually connected, nor are they connected to the Internet?

Mr. APPEL. That's true for many kinds of touch screen voting machines, but not for all kinds that are in use today.

Mr. HURD. And, Secretary Kemp, I just want to clarify that. And I guess this question to you as your role as the vice chairman of the Association of Secretaries of State. There are no voting systems that connect to the Internet, correct?

Mr. KEMP. Well, Commissioner Hicks might can back me up on this, but I know our systems are not. I wouldn't want to speak for every State in the country, but I would feel very confident in saying the vast majority, probably all are not connected to the Internet.

Mr. HURD. Mr. Hicks, do you have any opinions on that.

Mr. HICKS. From what we've determined, no voting machines are connected to the Internet.

Mr. HURD. So let's take one municipality, one voting district. They probably have how many machines? Is there an average number, you know, 5 to 10, 5 to 25, in one voting location? Let's take a voting location.

Mr. KEMP. Well, I think in Georgia, it would depend on the jurisdiction. Certainly, in a precinct in Fulton County you could have, you know, I would say, over 100 machines. In a smaller, rural county, you may have 5 to 10.

Mr. HURD. And so, Mr. Appel, in that scenario, an attacker would actually have to have access to all 100 in the one county in order to manipulate the records?

Mr. APPEL. In Georgia, that's not the case. The machines used in Georgia have been demonstrated to be hackable through a virus that's carried on ballot definition cartridges, very much like the Stuxnet virus was inserted into nuclear centrifuges in Iran.

Mr. HURD. But in that auditing system, in the auditing of these machines, we look at that. Is that correct?

Mr. APPEL. I'm sorry. Can you repeat the question?

Mr. HURD. So in those machines that have that vulnerability in the auditing process, isn't that scanned? Don't we scan for that?

Mr. APPEL. It's difficult to scan for that vulnerability in the sense of if you ask a machine to report what software is loaded in it, if it's fraudulent software, it will lie. So the AccuVote TS machines used in Georgia and in a few counties in other States are particularly vulnerable to this kind of virus that can be carried to the machines even if the criminal attacker doesn't touch the machines or is not even in the same State with the machines. The touch screen voting machines used in most other States, I don't know of any such way to hack them through a virus carried on cartridges.

Mr. HURD. Dr. Ozment, do you have any opinions on that? And when you provide best practices and information sharing to folks that request your assistance, is this the type of vulnerability that you all notify folks of?

Mr. OZMENT. You know, I think it's a good opportunity for me to elaborate on my answer. First, we have to always be vigilant. In the field of cybersecurity, we can never relax. We have no indication that adversaries are planning cyber operations against U.S. election infrastructure that would change the outcome of the election in November. And we have overall confidence in the system.

You know, individual parts of the election system are more or less vulnerable. You can never eliminate all vulnerabilities, but the overlapping layers of the system are what give us confidence, the fact that there is a wide variety of machines in use, a wide variety of procedures across jurisdictions, many checks and balances, physical controls, and the devices are not connected to the Internet.

So I cannot speak to the security of an individual device. What I can speak to is that, overall, we view the security of the overall system as robust. We can never relax obviously, and that's one reason that we are offering voluntary assistance to State and local governments.

Mr. HURD. Thank you, gentlemen.

Now I'd like to recognize the gentleman from California, Mr. Lieu, for 5 minutes of questions.

Mr. LIEU. Thank you, Mr. Chair.

Earlier this year, Donald Trump asked Russia to hack an American citizen. We know from later media reports that Russia has hacked the Democratic National Committee, as well as the Democratic Congressional Campaign Committee, and other entities for the purpose of influencing American elections.

And my question for you, Dr. Ozment, is what steps is DHS taking to try to prevent Russia or other foreign entities from influencing the American election this November?

Mr. OZMENT. Thank you. Without speaking as to the source of the intrusions into the DNC and DCCC, I do want to talk about some of what we're offering to State and local government officials.

First, we're offering them best practices. For example, we recently published a document on best practices for securing voter registration systems. We're also offering to scan their Internet-connected systems. So voter registration systems primarily, possibly tabulation for results reporting, and we're offering to scan these regularly for any vulnerabilities. And we will provide a weekly report on any vulnerabilities we detect and recommendations for mitigating them. We call that cyber hygiene scanning.

We're also offering to do more in-depth risk and vulnerability assessments. That would require us to send people onsite to do a much more detailed assessment of systems. We have local field-deployed personnel called cybersecurity advisers and protective security advisers. These individuals are available to provide assistance and advice to State and local governments.

And then finally, we've offered physical and protective security tools, training, and resources. All of those are available to State and local government officials. And then, of course, more broadly, we have the multistate ISAC, an entity that we have funded for well over a decade to help support State and local governments in their cybersecurity practices.

Mr. LIEU. Thank you.

Commissioner Hicks, thank you for your testimony. My understanding, from the main thrust of your testimony, is that because we've got 50 States, thousands of different jurisdictions, the American elections system is complex, diverse, and robust, because it's really hard to hack all of that. My view is they don't have to hack 50 States. In a close Presidential election, they just need to hack one swing State, or maybe one or two, or maybe just a few counties in one swing State. So I do sort of challenge your premise that just because we've got 50 States, somehow we are robust.

And my question is, is there a focus on these swing States to make sure that in States that potentially are close, that we do everything we can to make sure that the integrity of the elections are protected?

Mr. HICKS. Thank you for that question, Congressman. The EAC and the rest of the election community is focused on all the States, not just the swing States, because we feel that all the votes are valuable in that sort of realm. The basic premise of this is that if someone goes into a polling place and attempts to influence the election, that's still a Federal crime, and they should be prosecuted. So we're basically asking for people to serve as poll workers so they can be vigilant and serve as people who are on the front lines of seeing these sorts of things.

But to answer your question, you would still need a tremendous amount of people to go into any polling place to try to influence an election that way, even if it could be done, and we don't believe that it can be done.

Mr. LIEU. Thank you. As a recovering computer science major, I keep in mind that folks hacked computers well before the existence of the Internet, and we've had troubling reports of how these voting machines can be hacked quite easily.

And, Mr. Appel, you, yourself, hacked a voting machine. Are you aware of Symantec also hacking voting machines?

Mr. APPEL. Who?

Mr. LIEU. Symantec Corporation.

Mr. APPEL. No.

Mr. LIEU. For research purposes.

Mr. APPEL. No, but—

Mr. LIEU. Okay. Then let me just put this in for the record so people understand. So there was a Bloomberg article dated September 19 saying, "States Ask Feds for Cybersecurity Scans Following Election Hacking Threats." I'm just going to read this.

"In a recent simulation, Symantec Corporation said its workers were able to easily hack into an electronic voting machine. It was possible to switch votes as well as change the volume of data, said Samir Kapuria, senior vice president and general manager of Symantec's cybersecurity group."

And, Mr. Chair, if I could enter this into the record.

Mr. HURD. Without objection, so moved.

Mr. LIEU. Can you explain how you hacked the machine and if there's any reason why we would want a machine with no paper ballots? Wouldn't we always want a backup in case something was hacked?

Mr. APPEL. Yes. I'll be happy to explain. The machine that I hacked is called the Sequoia AVC Advantage. It's now called the Dominion AVC Advantage. It's in use in almost all of New Jersey and in all of Louisiana and a few counties of Pennsylvania and other States.

The computer program that counts the votes on this machine is in a read-only memory that's mounted in a socket on the motherboard. To hack this machine, you have to remove that memory chip from its socket and install a memory chip on which you've prepared a cheating program. The cheating program that I prepared has an extra 100 lines of code basically that when the polls are about to close, it goes in there and changes some votes stored in the machine. And there is an electronic log of all votes cast, so it changes the log too.

So to install that, the attacker doesn't need to be a computer scientist. The attacker just needs to have a bunch of copies of this memory chip with the program on it. And for each voting machine, unscrew 10 screws to remove the panel that covers the motherboard, pry out the ROM chip containing the legitimate program, and install the ROM chip containing the fraudulent program.

Other kinds of voting machines store their computer program that counts the votes in flash memory, and this can be updated under the control of whatever computer program happens to be running in the voting machine. These voting machines, typically the generation developed in the 1990s and after, can be hacked without actually physically changing any hardware in the machine just by installing a software upgrade memory card in the same slot that one would normally install the ballot definition.

And this particular attack was demonstrated by my colleague at Princeton, Professor Felten, in about 2007, working with two of his graduate students. But it's not just us at Princeton. There are many kinds of voting machines, and the same kinds of hacks are applicable to all voting machines and have been demonstrated at several other universities, including the University of Connecticut, Johns Hopkins, Michigan, and others.

Mr. LIEU. Thank you.

Mr. HICKS. Congressman, can I just add a little bit to this? One of the things I want to make sure that it's clear and when the Help America Vote Act came about, is that one of the reasons that the paper trail is not universal is that it doesn't allow for people with disabilities to basically be able to verify their vote and handle that paper. So someone who has a dexterity disability is not able to use that. But there are machines that allow for verification of ballots and are able to be used by those with disabilities.

So if Congress decides in the next session to look at reforming the Help America Vote Act, I would really encourage to make sure that the folks with disabilities are not left behind with the paper trail issue.

Mr. LIEU. Can I just briefly respond? You know, we launched a rocket, delivered payload to space station that landed on a barge. They've designed voting machines that actually you can have both a paper ballot and some sort of electronic input and have both. So it's not like it can't be done, and my understanding is L.A. County is about to do that. So my hope is that we don't have any more machines without paper ballots. Thank you.

Mr. HURD. Thank you.

I'd now like to recognize Congresswoman Kelly for her line of questions.

Ms. KELLY. Thank you so much. I mentioned in my opening statement about hackers attacking the voter registration databases in Illinois and Arizona. So I'd like to take a moment to understand what these attacks are and what they are not.

Dr. Ozment, was the cyber attack on the voting machines or was it on voter registration databases?

Mr. OZMENT. Thank you, Representative. The cyber attacks that you're referring to in Arizona and Illinois were attacks on voter registration systems, and they seem to have been intended to just copy the data on those systems, possibly for the purposes of selling

personal information. So we have not seen intrusions intended to in any way impact individuals' votes in actual voting.

Ms. KELLY. Why are these more vulnerable than the actual machines?

Mr. OZMENT. Voter registration systems are more commonly connected to the Internet, in part to ease that registration process, and so because they are connected to the Internet, they are obviously more susceptible to cyber intrusions.

Ms. KELLY. And it seems like all of you in various answers are saying that it would be difficult for a hacker to succeed in accessing the U.S. election system and rigging the results in an undetected way, that you all seem to feel like that. Is that correct?

Mr. OZMENT. That's correct. Because of the different layers of security in the system, even though individual parts of the system may be vulnerable, we overall have confidence in the system.

Ms. KELLY. And what is DHS doing to help States secure these databases?

Mr. OZMENT. We recently released a best practices document focusing particularly on voter registration systems to help States secure those systems. Also, our cyber hygiene vulnerability scanning that we offer to States will be particularly helpful for those systems because many of them are Internet connected. So we have a whole host of resources available to State governments that are applicable both to their voter registration systems and to other systems, even systems outside of the voting process.

Ms. KELLY. And is it correct there are at least 40 States with the network defense device similar to the Einstein censor used by Federal agencies?

Mr. OZMENT. The majority of States—I don't know the exact number—absolutely take advantage of a service that we offer through the MS-ISAC, which provides network protection for those States.

Ms. KELLY. And is it at the same protection level as the Federal? Is the State as good as the Federal?

Mr. OZMENT. You know, it's a different capability than the Federal system, just suited to the networks that State and local governments offer. There's one key difference. One of the Federal systems can take advantage of classified information that is not currently available through the multistate ISAC for State and local governments. We have made that available in a different way for State and local governments.

But what I can say is overall we have made all of those protections available to State and local governments through one mechanism or another.

Ms. KELLY. And, Mr. Hicks, what is your agency doing to help States secure their election systems?

Mr. HICKS. If we're talking about voter registration systems, one of the things that I would like to include in the record is the EAC has a checklist for securing voter registration data, and that lists out a number of things, basically, from access control to auditability to making sure that we document everything and everyone who has access to that system. And I would like to make that available for the record.

Mr. HURD. Without objection, so moved.

Ms. KELLY. And, Mr. Norden, can you briefly describe how voting machines are vulnerable and how widespread the problem is?

Mr. NORDEN. Yeah. Well, I would echo the comments that were already made about the fact that because voting machines aren't on the Internet, that certainly is an important distinction to be made between machines that we're voting on on election day and things like a registration database, which is generally connected to the Internet.

In terms of vulnerabilities, again I would say my concern mostly is about, for voting machines, is mostly about the fact that this equipment around the country is getting very old, and as the equipment gets older, we are more likely to see failures. We see things.

And, again, I am particularly worried about this in the age of social media. We saw this a little bit in 2012, but with touch screen machines, there are often, as machines age, more calibration problems. In Virginia, there was an instance where the glue between the screen and the machine itself was just degrading, and as a result, the kind of thing that happens is somebody—I'm sure you've seen the videos of this before—somebody selects one candidate, another candidate shows up. I think that's not very good for voter confidence. And when that's posted on YouTube, as it inevitably is, the more and more that we see of these things, again, especially in the context of hearing about hacks to voting systems, that can be a very dangerous thing. And that machine has to get taken out of service.

You get long lines. There was a study from researchers at Harvard and MIT that estimated between 500,000 and 700,000 people were not able to vote in 2012 because of long lines. I think that's a huge risk to the integrity of our elections.

Ms. KELLY. This might just be a guess on your part, but how—or if anybody else knows—how old are the oldest machines that are still being used?

Mr. NORDEN. They're probably among the oldest in New Jersey. I would say, actually, ironically, I think some of the oldest machines probably have less of a need of replacement than some of the newer systems that we bought, because systems particularly bought just after the Help America Vote Act was passed that were designed in the '90s are essentially laptops from the 1990s, and those were not built to last much longer than 10 or 15 years.

Ms. KELLY. Dr. Appel, anything to add?

Mr. APPEL. Yeah. I think some of the oldest electronic voting machines in use in this country date from the late 1980s. Some of those machines are still reliable in the sense of not breaking down. My concern with the machines is more, you know, can they be hackable without a paper trail that could let you recover the correct result of the election?

Mr. HICKS. Congresswoman, one of the things that the EAC is doing now is we're working on our next iteration of our voluntary voting system guidelines. And so these guidelines will be an update since the last ones, the last full ones that were done, which were done before the iPhone was invented. So we want to make sure that we incorporate the new technologies that are here today in looking towards tomorrow. So we're asking for anyone to join our public working groups to give their input to make sure that the

next standards that we do are basically the best standards we put out.

Mr. KEMP. I would just add, I know we've been kind of singled out with our voting equipment being fairly old, early 2000s, but I would just remind the Representatives that this isn't equipment that we're using every day like you use your phone or your laptop or your desktop. This is equipment that's used two or three, maybe four times a year. We have policies and procedures in the State where the counties have certain ways that they have to care for the equipment, and they have held up well. So I think it's just important to realize that as well.

Even though the technology may be old, it doesn't mean it's bad, and the equipment is wearing well. We actually do an assessment after every election, the Center for Elections at Kennesaw State does. We have a less than 1 percent failure rate on our elections equipment. So, you know, if that changes, that will certainly raise a red flag to us, but right now we have not seen that.

Ms. KELLY. We have made it a point—I'll give him the credit—of not just having hearings to have hearings. And we always ask how can Congress help make things better. But where do you think—and any of you can answer this—where should the priority be in investing in our election systems to make sure they're secure and the public does have the confidence, and how can Congress help?

Mr. HICKS. I spent 11 years as a staffer here on the hill and I know the difficulty that Members face in terms of making sure that things are done correctly, but also having a financial responsibility to that. I think that my role now at the EAC is one to give Congress as best advice as I can to move things forward.

And so, you know, in my own opinion, I'm looking at voting machines like a fire truck. Fire trucks are still going to be out there. They need to be used. They need to be—you know, if there's a fire, they're going to have to be used. But until a new fire truck can be purchased, you have to use that old one. And so what can you do? And so what we're doing at the EAC is making sure that we give the best guidance in terms of managing those things. So on our Web site we have 10 things to do on managing aging voting equipment.

And so in the future, I would say that if Congress wants to look at this to look at how much will it cost to replace these machines if we're going to do that, but also to look at other aspects of it. To say, you know, do we want to start talking about this third rail of, you know, using our own devices to cast ballots and things like that. But also we want to make sure that we look at military and overseas voters as well because they don't have these same options of using the equipment that we have here, and looking at disability groups, but also looking at our aging population as well. So there's a lot of things, and I would be happy to come up here any time to discuss any of those topics.

Ms. KELLY. Anything?

Mr. KEMP. Well, I think—that's a really good question, by the way, and I think there's a couple of things that come to mind for me. I would encourage Congress to let the States remain flexible in what systems that they're using. I think there's great value in

that. I know the National Conference of State Legislatures agree with that assessment as well. But I would also urge you to work with the National Association of Secretaries of State.

I know Commissioner Hicks and his colleagues have been to many of our meetings, winter meetings that we have in D.C., and I think I can pretty much 100 percent speak on behalf of the organization that we'd love to have any Member of Congress or even do maybe a session during that winter meeting where you can hear a different perspective, because it is different. I mean, one size does not fit all in elections. What we're doing in Georgia is going to differ greatly from what, you know, Jim Condos may be doing in Vermont, or what's going on in California, and we would welcome and encourage that.

Ms. KELLY. I used to be a State rep, and I know Jesse White really well.

Mr. HURD. Thank you. And the chair notes the presence of our colleague, Congressman Jody Hice, from Georgia. We appreciate your interest in this topic and welcome your participation today.

And I ask unanimous consent that Congressman Hice be allowed to fully participate in today's hearing.

Without objection, so ordered.

And, Mr. Hicks, I know you have a time deadline, but I think we should be done by that deadline, but I'd like to now recognize Congressman Hice for 5 minutes.

Mr. HICE. Thank you very much, Chairman. I appreciate you letting me be a part of this.

And, Secretary Kemp, I just want to say hello to you. It's always great to have some Georgians up here, and it's an honor to have you, sir. Thank you for participating. And all our witnesses today, thank you for being here.

Secretary Kemp, let me just go with you. The broader question here, of course, that we are all concerned about and well should be is that of voter fraud, regardless of how it shows its face. Can you explain some of the steps that Georgia has taken in particular to prevent voter fraud across the board?

Mr. KEMP. Well, thank you, Congressman. It's great to see you as well as Representative Carter.

We have really done a lot. I know I've spoken a lot about our voting system not being connected to the Internet. We have got all kind of policies and procedures about how we tie the number of votes on a specific machine that is counted with our paper tape inside the machine back to the signed voter verification of the voter when they come in the precinct. So I want to assure people that there is a way that we can tie that down.

But we've also seen, and it hasn't really been talked a lot about here today, but, you know, there's fraud that happens with paper ballots as well. We've seen it in many local jurisdictions with absentee ballots. We've had elections that have been overturned because of things of that nature, people manipulating the paper absentee ballot process in Georgia, especially in a local election, a municipal election, where, you know, literally 5 to 10 votes could sway an election.

But one of the things that we've done in Georgia, I think, besides having really good State laws and State election board rules on

how the counties should handle the statewide voting system and training in that regard to protect the integrity of the election, we've also, as Commissioner Hicks said earlier today, we've asked for the public's help, not only as poll workers or poll watchers, but we've got a stop voter fraud hotline and an email that we monitor.

Unlike some other jurisdictions across the country, we actually have a law enforcement division in the Secretary of State's office. Any complaint that we get, any complaint, it can be something as serious as potential vote buying, to something maybe as small as there's a handicap lift that wasn't working correctly at a precinct or there's not enough parking or there's long lines, we'll respond to every single one of those cases or look into those to see if it warrants an investigation.

So we encourage Georgians that may see something improper, if they feel like their vote hasn't been cast properly, if somebody was manipulating them in a precinct, whatever it is, to report that to us, and we strategically put our investigators and inspectors around the State during the early voting advance period and on election day where we can respond very quickly. So we have a lot of ways that we try to stop voter fraud.

But contrary to some people not believing it happens, it actually does. And when that does happen, we bring those individuals or counties, if they're not following the rules and procedures, to the State election board, and we have a due process that we go through. And we've actually had, you know, candidates that have paid heavy fines and have committed to never run for office again because of the actions that we've taken. So that's something, you know, and we treat every case the same, you know, when it comes to that.

Mr. HICE. What about specifically when it involves electronic voting machines? I'm sure there are glitches from time to time. When someone offers a complaint due to a machine, what's your process?

Mr. HICKS. Well, as you can imagine, that's something that's high on our radar, so we'll send somebody out. I mean, if we have an equipment problem, there's a couple actions we can take. We can send an investigator. We have emergency preparedness plans where, especially on big elections like we'll be having November the 8th, where we've coordinated with State Patrol and Department of Public Safety to have a helicopter and a trooper at the Kennesaw State election center.

So let's say we have a server go out, which we had happen in a county. You know, if you don't get on that quickly and the results don't come in quickly, then the public starts to ask the question, why is that happening? So we now have the ability to either fly or drive with a law enforcement official, equipment. Or we've had times where we've had a failure with the voting equipment. We've had to send a technician out there to help maybe get a memory card out of there or something of that nature.

So there's a lot of steps that we take to investigate, you know, also before the election to prevent those things happening, but also to make sure public confidence stays intact by responding quickly to those type things.

Mr. HICE. Thank you, Mr. Chairman. I yield back.

And, Mr. Secretary, thank you. Always great to see you.

Mr. HURD. I'd like to now recognize my friend and the Congressman from the great State of Georgia, Buddy Carter, for his 5 minutes.

Mr. CARTER. Well, thank you, Mr. Chairman, and thank all of you for being here. This is obviously a very important subject that all of us are concerned with.

Secretary Kemp, again, it's good to see you. Thank you for being here. Thank you for your work in the State of Georgia. We appreciate all of your efforts in making sure that our elections are run in a safe and effective manner, and you're doing a great job and we appreciate it. I appreciate the opportunity to have worked with you in the General Assembly and have fond memories of that.

I wanted you to provide us some insight in your position as Secretary of State—and you also, as I understand, serve as co-chair of the National Association of Secretaries of State's Election Committee, and also as a member of the new DHS Election Infrastructure Cybersecurity Working Group. Cybersecurity is something we talk a lot about up here. I also, as the chairman also, he and I both serve on Homeland Security, and we are very concerned about cybersecurity.

Mr. Secretary, can you briefly describe your role as a member of the DHS Election Infrastructure Cybersecurity Working Group? Can you tell me basically what you all do?

Mr. KEMP. Well, it's a relatively new task force, if you will, that was created by Secretary Johnson and DHS so that we can have collaboration between the States and the Department of Homeland Security, and I certainly applaud that. I've had some people ask me why I would serve on that when I was so critical of the critical infrastructure definition, but I do. I feel very strongly that that's a designation that should not be put on election systems, but I also feel strongly that there are ways that we can collaborate as Secretary of State or State elections officials with a lot of different branches of the Federal Government to make sure that we're prepared, that we're informed, and that we can better protect our system.

So the Working Group right now really has just been a series of phone calls to go over what DHS has rolled out for States that need or may want to voluntarily take advantage of some of the things that have been talked about, the cyber hygiene scanning and other things. And right now, from all I know, unless we have some sort of other event pop up, that's probably about all that's going to happen before the election, other than the States knowing that they can reach out to DHS directly.

From the State of Georgia's perspective, we're already doing a lot of the things that have been offered, so we don't have the need for the assistance. It's not that we're not grateful for it being out there, it's just something that, you know, thankfully, we have been working on this issue, like you were saying, cybersecurity, for 3 years. And I know all of State government has as well. And we see that every day, not only in the Secretary of State's office, but all across State government in the State of Georgia, and we're part of an information sharing analysis center as well in Georgia that's going through the Technology Authority, GTA.

Mr. CARTER. Okay. Let me shift gears here for just a second. It's my understanding, the U.S. Election Assistance Commission, it's my understanding that the National Association of Secretaries of State has called for the elimination of that on several occasions. In fact, just recently, the most recent I should say, is probably in July of 2015. As the Secretary of State of Georgia, have you had any interactions with the EAC?

Mr. KEMP. I have. You know, I was one of those, for full disclosure, that supported a resolution. I think it was several years ago. Mr. Hicks may have a better memory of that than me, because I felt like the usefulness of the organization, the time had passed. But to answer your question, yes, I have had dealings with the EAC. They're part of this working group, and I will say they've been very responsive in their role.

Mr. CARTER. So have they improved? I mean, are you now—do you now think that they're beneficial?

Mr. KEMP. Well, I wouldn't want to go that—well, I definitely think they're beneficial. I have different thoughts about that that maybe in another setting I could spell out a little more detailed. But they've certainly been responsive in this issue.

Mr. CARTER. So should we eliminate them or should we just transfer some of that work to another group?

Mr. KEMP. I'm of the belief that we can do a lot of that at the State level.

Mr. CARTER. Mr. Hicks—

Mr. KEMP. But I want to say it's been—I've been grateful that we have commissioners that have now been appointed to the EAC where they can work on certain things that are required at this time.

Mr. CARTER. Mr. Hicks.

Mr. HICKS. I want to thank Secretary Kemp for his support. One of the things, when I—one of the reasons I spent 11 years up here was I spent 4-1/2 years as a nominee waiting for my confirmation.

Mr. CARTER. Four-and-a-half years?

Mr. HICKS. I'm the longest serving Obama nominee, and I was finally confirmed in December of 2014.

Mr. CARTER. Who does the confirmation?

Mr. HICKS. The Senate Rules Committee. But it was the full Senate.

Mr. CARTER. We're doing all we can. I feel your pain. We have to deal with them too.

Mr. HICKS. But overall, the Election Assistance Commission sat without commissioners for almost 3 years and then sat without a general counsel or an executive director, so a lot of that work wasn't getting done. So when my fellow commissioners and I were confirmed, we hit the ground running. And so I think that, you know, most of the Secretaries of State have changed their tune to figure that we are more valuable now.

But our role is to the States and locals and other stakeholders like the voters themselves, and so I think that now we are proving that we are valuable and hopefully will continue to do that.

Mr. CARTER. Well, great.

Again, gentlemen, thank you for what you do. This is extremely important, and we all recognize that and all appreciate your work and your diligence in this.

Thank you, Mr. Chairman. I yield back.

Mr. HURD. The gentleman yields back the balance of his time.

I'd now like to recognize the ranking member, Mr. Cummings.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

This summer, there were reports that Russia was attempting to compromise our elections by hacking into election systems. This is a very grave issue that threatens the foundation of our democracy. On Monday, Ranking Member Diane Feinstein in the Senate Intelligence Committee and Ranking Member Adam Schiff of the House Intelligence Committee issued a joint statement. They said, and I quote, "Based on briefings we have received, we have concluded that the Russian intelligence agencies are making a serious and concerted effort to influence the United States election," end of quote. They issued the statement after careful consultation with the intelligence community, our intelligence community.

Now, Dr. Ozment, I assume you have no reason to question the accuracy of this statement. Is that right?

Mr. OZMENT. Sir, the executive branch has not attributed these incidents to any entity, and the FBI is leading an ongoing law enforcement investigation of these breaches.

Mr. CUMMINGS. Here is what I don't understand. For some reason, Donald Trump keeps defending Russia against these hacking allegations. In fact, in Monday night's debate, he said he doesn't know if it was Russia. It could be China. It could be a 400-pound person in bed, he said. Frankly, his statements seemed ridiculous to me. Not only has Mr. Trump defended Russia, he has encouraged Russia to conduct the hacking.

Dr. Ozment, DHS plays a key role in helping States protect their election systems against cyber attacks. Is that right? Is that right, sir?

Mr. OZMENT. Sir, we are there to support State and local governments in defending their systems. That's right.

Mr. CUMMINGS. Well, this morning, FBI Director James Comey told the House Judiciary Committee, and I quote, "There's no doubt that some bad actors have been poking around," end of quote.

Here's my question, without disclosing any classified information, have you seen any uptick in probing attacks by foreign adversaries over the past 3 months?

Mr. OZMENT. Sir, I don't think we have a concrete answer for that question. What I'll tell you is, obviously, you know, there are two incidents in Arizona and Illinois that resulted in breaches of voter registration systems. And what I'll say applies only to voter registration systems and, therefore, does not impact the actual casting of a vote.

As part of our response to that, we and others in the Federal Government have shared information with State and local governments, essentially Be on the Lookouts, which are called cyber indicators. State and local governments are using that to more carefully monitor their systems. Any time you more carefully monitor a system, you're going to see more bad guys poking and prodding at it, because they're always poking and prodding. What I can tell

you is that I think it's safe to say that voter registration systems that are online will always be the subject of interest from bad guys, whether for stealing personal information by criminals or other nefarious purposes. And that's why we think it's important that State and local governments constantly focus on the security of those systems, and we have published guidelines to help them secure those systems.

Mr. CUMMINGS. On August 30, 2016, I sent a letter with ranking members of the Committees on Judiciary, Foreign Affairs, and Homeland Security, asking whether the FBI is investigating troubling connections between members of the Trump inner circle and the Russian interests.

I ask unanimous consent that this letter be made a part of the record, Mr. Chairman.

Mr. HURD. Without objection, so ordered.

Mr. CUMMINGS. Dr. Ozment, earlier this morning, FBI Director Comey was asked about this letter before the House Judiciary Committee. Comey said that the FBI is trying to figure out, quote, "just what mischief is Russia up to in connection with our election." He also said he would not inform Congress, at least at this stage, about any interviews with individuals working for Mr. Trump who were listed in this letter, because he does not comment on ongoing investigations.

I want to ask you specific questions about this, but generally, does DHS work with the FBI to investigate illegal acting by foreign adversaries?

Mr. OZMENT. So, in July, the President released Presidential Policy Directive 41 that laid out the role of DHS and the FBI in investigating cyber incidents. And you can think about it as a significant cyber incident being the equivalent of an arson in the real world. And when you have an arson, you want both the firefighters and the cops to show up. In this analogy, the FBI are the cops. They're the lead what we call threat responders, the lead law enforcement agency. My organization are the lead firefighters. So we focus on helping the victim and taking information to share with other victims and help them—or other potential victims and help them protect themselves. So we do collaborate closely with the FBI, but it's the FBI in the lead role for ascertaining who is the perpetrator and bringing that perpetrator to justice.

Mr. CUMMINGS. One last question: Again, generally, if you come across evidence that anyone in the United States was aware of these illegal actions or even collaborated with foreign adversaries, would you work with prosecutors and FBI investigators?

Mr. OZMENT. If at any time we come across any evidence of a crime, unless we are prohibited from sharing that, we would immediately share it with law enforcement agencies.

Mr. CUMMINGS. Chairman, I yield back. Thank you.

Mr. HURD. Thank you, Ranking Member.

And, Mr. Hicks, I want to say thank you for your time and contribution to this hearing. I know you have to slip away, and if you do, please go ahead.

Mr. HICKS. I can't leave when my own Congressman just showed up. So I don't know if I—I can take the 5 minutes to see if he has questions for me.

Mr. HURD. Great.

Well, with that, I would like to recognize my friend from the Commonwealth of Virginia, Mr. Connolly, for 5 minutes.

Mr. CONNOLLY. I know Mr. Hicks is not flying home.

Mr. HICKS. I'm actually going to Iceland.

Mr. CONNOLLY. My daughter was just there. She was hiking.

Thank you, Mr. Chairman.

And thank you to the panel.

And good luck, Mr. Hicks. Enjoy Iceland.

Last month, the Department of Homeland Security Secretary Jeh Johnson said, and I quote: "We should carefully consider whether our election system, our election process is critical infrastructure, like the financial sector, like the power grid."

Mr. OZMENT, what did Mr. Johnson mean by that?

Mr. OZMENT. So, first, I should note that DHS has not formally designated the electoral system as critical infrastructure. We are focused right now in the immediate term on providing whatever resources and assistance we are able to provide to States and local governments and whichever resources and assistance they want from us.

You know, longer term, I think that's a conversation that we want to have with State and local governments. Under our authorities, there are additional capabilities that we can provide to those governments if we designate the system as critical infrastructure. That includes additional protections we can put on information. If, for example, we wanted to get in a conversation with both State and local governments and vendors, we could better protect the information that those vendors provide to us. We have—we can better prioritize the resources that we want to give to them, and it improves our ability to, for example, offer clearances to folks involved in this process.

I would like to highlight that if we were to make that designation, it does not give us any regulatory powers. All of our resources and assistance would still be voluntary, you know, and the State and local governments would remain in charge of elections.

Mr. CONNOLLY. So if, however, we did declare it critical infrastructure, I think Mr. Appel said there were 12 States that still use touchscreen technology. Is that correct?

Mr. APPEL. Some States use touchscreens in some of their counties and not others. So I said approximately 10 States, based on the preponderance of the use of—

Mr. CONNOLLY. So if we declare it critical infrastructure, we might be able to provide some assistance if those States chose to move to the, you know, paper/electronic kind of ballot.

Mr. OZMENT. We can offer assistance now, and I think it would help us in our ability to offer assistance. But we would not, for example, be able to replace their systems. We wouldn't be able to offer that type of assistance.

Mr. CONNOLLY. Mr. Kemp, I want to make sure I understood your testimony. I thought I heard you say that elections should be governed strictly by States and localities and that it was not really the business of the Federal Government. Am I getting your testimony correctly?

Mr. KEMP. Well, it's a constitutional duty of the States to run elections.

Mr. CONNOLLY. Isn't also, however, a concern of the Federal Government that Federal elections have some uniformity to them? For example, the Voting Rights Act.

Mr. KEMP. Well, I certainly understand your point, but I think the whole argument of critical infrastructure, just like Mr. Ozment just said, protecting vendors' information really goes against the open process that we have now at the State level where, like when we test our voting equipment, it's advertised in the local legal organ. You know, the local newspaper editor or reporter can come watch that process that the local election boards do, and any citizen.

And I think the idea of federalizing our elections to where we have a one-size-fits-all voter registration system or mandating that States use a certain voting system or one type of voting system creates all kinds of problems and, quite honestly, I think would make our system—make the system more vulnerable, not less.

Mr. CONNOLLY. Well, so are you saying that, from your point of view, the 50 different State systems plus tens of thousands of localities is just fine, and we shouldn't even look at it at the Federal level?

Mr. KEMP. Well, I wouldn't say that you shouldn't look at it and everything is just fine. There's certainly jurisdictions out there that do better than others. We have that in the State of Georgia. But I believe that we're better suited as a State to provide solutions for that than the Federal Government is.

Mr. CONNOLLY. Well, what about the Voting Rights Act? I mean, that was an argument used back in the 1950s and 1960s for the Federal Government to keep its nose out of State jurisdiction. Frankly, if the Federal Government hadn't passed the Voting Rights Act, people would have still been disenfranchised, including in your home State and mine.

Mr. KEMP. I would say that the Voting Rights Act is still intact.

Mr. CONNOLLY. Yes, but it's an example of the opposite of what you're asserting. It was an example of federalizing something to protect the franchise, because the States weren't doing it. In fact, States were actively suppressing votes. You don't deny that, do you?

Mr. KEMP. Well, I'm not sure I understand what that has to do with the election system.

Mr. CONNOLLY. Well, I'm dealing with your assertion of the principle that we shouldn't federalize any aspect of this. And I'm arguing that the Voting Rights Act is a clear exception to your principle and that perhaps the Federal Government in Federal elections, at least, has an interest that overrides the State interest when it comes to protecting, at the cyber level, the integrity of the results.

Mr. KEMP. Well, that's certainly your opinion. Mine differs.

Mr. CONNOLLY. I yield back, Mr. Chairman.

Mr. HURD. Thank you, Mr. Connolly.

I now would like to ask unanimous consent to submit two letters for the record: One from the National Association of Secretaries of State. It is an open letter from the Nation's secretaries of state to Congress talking about how we can work together to share the

facts about cybersecurity in our elections. The second letter is from the Electronic Privacy Information Center about this hearing.

Without objection, so ordered.

Mr. HURD. Mr. Hicks, one of the things that you said, one of the three points that the EAC is responsible for is providing grants. Is there grant money available to help upgrade aging equipment?

Mr. HICKS. Most of that money has already been accounted for, so there is no money available to replace voting equipment.

Mr. HURD. Thank you.

And, Dr. Ozment, I just want to be clear. This conversation about designating voting systems as critical infrastructure, that is off the table for this election. Is that correct?

Mr. OZMENT. It's not what we're focused on in the near term. We really in the next 3 months—voting has started. You know, voting is occurring in a number of jurisdictions across the U.S. For the next few months, we're focused on how we can help State and local governments.

Mr. HURD. And I would like to end with my takeaways from this, is that pieces of our voting system are vulnerable, but it's really hard to hack our voting systems. There are some that need to be upgraded. We should never rest on outdated legacy systems and that we should be looking at how we solve this problem working together and that there's resources within DHS for our States to voluntarily ask for. And this is not forcing any particular program on an individual State.

And what I'd like to do in my remaining 3 minutes, I'd love to go down the line and everybody take 30 seconds and give your final points. This is an important topic. I appreciate you all being here, and this is your last conversation with the American people.

So let's start with you, Mr. Norden, and work our way backwards.

Mr. NORDEN. Thank you, Chairman Hurd.

I guess I would emphasize two things. What I said earlier, I think, one of the most important things that we can do is ensure that there is confidence in the system. I think that the issues of access and confidence and integrity of our voting system are all interdependent and linked. Too often, access and integrity are presented as oppositional.

I do think that there is a role for Congress after this election to start thinking about what investments the Federal Government can make to ensure that there is confidence in the system, through research grants for innovation and for replacing some of the oldest equipment that really is a challenge.

And one last point I want to make is, because so many States are leaving it to counties to purchase this equipment, we really are starting to see a kind of two-tiered system in this country, with counties with less money, less resources—they're often rural counties—are left without being able to invest and replace their equipment. And we're talking, yes, about local elections but also Federal elections, of course.

Mr. HURD. Thank you, Mr. Norden.

Mr. Appel, 30 seconds.

Mr. APPEL. After the election, I think it would be a very good thing for the Congress to find a way to assist and encourage those

10 States that still primarily use paperless touchscreen machines to switch to optical scan machines. I would say also that there are many safeguards in our American elections which we haven't explicitly discussed in this hearing, and those have to do with the inherent transparency of the canvassing process in many States, in most States, where the results are announced in each precinct of how many votes each candidate got in the precinct. And the challengers, the party challengers, and any interested citizen can see for themselves that those numbers add up to what the election officials are reporting in the precinct-by-precinct totals. And that's a safeguard against hacking of the computers in county central that might be adding up those precincts.

So we should encourage measures that election administrators are already taking to make transparent the process of reporting the precinct-by-precinct numbers in a way that we can see that they add up.

Mr. HURD. Excellent. Thank you, sir.

Secretary Kemp.

Mr. CONNOLLY. Would the chairman yield for one second?

Just to Mr. Appel's point, we had an election in Virginia for a State attorney general. And because we had a paper trail, we were able to see an anomaly in absentee ballots cast, that clearly there was an anomaly in one congressional district. And sure enough, there was a ballot box that had accidentally been put aside because of a malfunction, and the votes had not been counted. It actually made the difference in terms of who won; it was that dispositive. So what Mr. Appel is saying I think is really critical in terms of getting accurate results in our elections throughout the country.

Mr. APPEL. I'll just add that the kind of transparency you get from that makes it so that you don't have to be a cybersecurity expert to understand that anomaly and correct it.

Mr. HURD. Secretary Kemp.

Mr. KEMP. Chairman Hurd, thank you for having me today, members of the committee. I appreciate the opportunity to be here.

I think, in my 30 seconds, I would just encourage you to continue to collaborate with the secretaries of states, Lieutenant Governors, and other election officials back home and ask them what they're doing, what they're doing to prepare. I would encourage all American citizens to do that as well. I think they'll be very pleasantly surprised to see the preparations that are going on all across this country to make sure we have secure, accessible, and fair elections in Georgia. And I certainly would appreciate any more collaboration that we can have with this committee or other Members of Congress and the National Association of Secretaries of State to work together in the future.

Mr. HURD. Mr. Hicks.

Mr. HICKS. Saturday marked the 45 days before the election, and on that day ballots were sent out to our men and women overseas so that they can start casting their ballots back. Early voting is going to start soon for many States. And one of the messages and the message that I want to make sure is clear today is that our elections are secure.

We on our Web site and throughout the Nation when we've gone around this country have talked about our Be Ready 16 campaign

to talk to States about how they can secure their elections, how to make sure that the ballots are being counted accurately and so forth. And, you know, come November 8, we know that we will have an election and that election will be secure.

Mr. HURD. Dr. Ozment.

Mr. OZMENT. We must be vigilant, as we must always be in an area where there are cyber threats. Particularly, as many States upgrade their voting systems over the next 4 years, we must build those systems to have more cybersecurity that stops not just the attacks of today but the attacks of the future, when they'll still be used in 2030 or 2040.

But overall and right now, we have confidence in the integrity of our electoral system. We have no indication that adversaries are planning cyber operations against U.S. election infrastructure that would change the outcome of this election. We believe that the diversity and many different levels of checks and balances in our electoral systems are sufficient that we should all have confidence in the integrity of the system and the election.

Mr. HURD. Thank you, Dr. Ozment.

Now I'd like to recognize Ranking Member Cummings for 5 minutes.

Mr. CUMMINGS. Thank you very much.

Again, I am concerned very much about the cyber situation, but I'm also concerned about African Americans and Hispanics and so many others who have been blocked from voting. I think that I will go to my grave trying to do everything in my power to make sure that everybody has an opportunity to vote. My foreparents were denied it over and over again, and I'm seeing a lot of the same things happening today.

Mr. Kemp, you are secretary of state for Georgia, which is one of the three States that were allowed to modify the Federal form to require proof of citizenship in your State, based on the unilateral decision of Brian Newby, the EAC Executive Director. I understand that you submitted a request for this modification. But in addition to that, did you or anyone in your office have communications with Mr. Newby or anyone else at the EAC relating to this request?

Mr. KEMP. I have to look back and see if that was the case before or after. I know we had written letters asking for this issue to be treated like the EAC had treated previous instances, where we could simply treat the Federal form the same way that we treat the State form in our State.

Mr. CUMMINGS. Can you please provide this committee with the copies of all email or other communications between you or anyone in your office and anyone at the EAC about this issue? Would you do that for us, please, sir?

Mr. KEMP. We can do that.

Mr. CUMMINGS. Thank you.

Mr. Kemp, what evidence did you submit to the EAC demonstrating that the modification you requested was necessary for the administration of elections in Georgia?

Mr. KEMP. Well, we were simply trying to, as I said earlier, match the State form with the Federal form.

Mr. CUMMINGS. Will you provide the committee with all documents relating to that issue also?

Mr. KEMP. We certainly can look into that.

Mr. CUMMINGS. No, that's not what I asked you. I said, would you provide us with the documents, sir?

Mr. KEMP. Well, I wouldn't be able to answer that question, but I can certainly look into that and get back to you.

Mr. CUMMINGS. I'd like you to provide to the committee any and all documents that you and your office have relating to any analysis you did regarding the impact on eligible voters that your request would have. Did you look into that?

Keep in mind in North Carolina what they did is they systematically figured out when black people vote; they figured out how they vote; and then they, with precision—with precision—made sure that they did everything in their power to stop them from voting.

And so I just want to make sure that we have the documentation. I'm sure whatever you did is proper, but I'd just like to know. It would be congressional malpractice on my part, as a son of people who could not vote, to sit here and have you all here and not address this issue. So I'd just like to have the documents. That's all. I'm sure you've got justification.

Mr. KEMP. Well, Representative, it's really a pretty simple thing that we were trying to do. We were simply trying to make the Federal form have the same questions as the State form.

But I will tell you, as the State of Georgia, under my administration and leadership, we have implemented online voter registration where anybody that has a driver's license or a State-issued ID card can register to vote 24 hours a day, 7 days a week. And we've had over 360-some thousand people that have used that system.

Right now, we have a Student Ambassadors Program that we started last year with a pilot of 14 high schools around the State and 150 kids. It's now ballooned to over 800 students in any kind of high school that you can imagine across the State of Georgia. We have over 102 high schools where we're actually teaching students in the school to register their peers to vote.

So I can assure you if anybody that meets the requirements and wants to register to vote in Georgia, they can easily do so.

Mr. CUMMINGS. I'm glad to hear that. I just have two more questions. The Court of Appeals for the D.C. Circuit temporarily halted and reversed the unilateral action by the EAC Executive Director. However, prior to that, do you know how many voters in Georgia had tried to register using the Federal form and were turned away because they did not provide proof of citizenship?

Mr. KEMP. I wouldn't be able to answer that question.

Mr. CUMMINGS. And how long will you need to get back to us on that? Can you get that information?

Mr. KEMP. I'll have to check on that and get back to you.

Mr. CUMMINGS. Mr. Chairman, as I said, I am just concerned. When Justice Ginsburg was talking about Texas, I think it was in the Shelby case, and she was saying that 600,000 Texans would not be able to vote, I mean, if we want to have an emergency, that's what the emergency ought to be about. Every single person, I don't care whether they're Tea Party, Green Party, Democrat, or Republican, I will fight for their right to vote.

And I just want to thank you, Mr. Chairman, for your courtesy. And I look forward to your responses, Secretary of State Kemp.

Mr. KEMP. Let me just make one point. While we were asking for the form to be changed, we never stopped taking the Federal forms.

Mr. CUMMINGS. But can you understand—and I'm almost finished, Mr. Chairman. But can you understand why African American people, Hispanics, and others might be upset when people are—I'm not saying you—when people are blocking them from voting, when they're paying taxes and working hard and doing everything they're supposed to do and not be able to vote? I mean, can you understand it?

Mr. KEMP. Well, I can understand it, but I can assure you that that's not happening in Georgia. Actually, we've seen minority participation increase in our State.

Mr. CUMMINGS. Thank you.

Mr. HURD. I'd like to thank our witnesses for taking the time to appear before us today.

If there's no further business, without objection, the subcommittee stands adjourned.

[Whereupon, at 4:54 p.m., the subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Congress of the United States
Washington, DC 20515

September 28, 2016

The Honorable Thomas Hicks
Chairman
U.S. Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

Brian Newby
Executive Director
U.S. Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

Cliff Tatum
General Counsel
U.S. Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

Dear Commissioner Hicks, Mr. Newby, and Mr. Tatum:

We are writing to follow up on our June 1, 2016, letter regarding Mr. Newby's unilateral decision as Executive Director of the U.S. Election Assistance Commission (EAC) to amend the federal voter registration form to require proof of citizenship in Alabama, Georgia, and Kansas.¹

We remain extremely concerned that Mr. Newby's actions violated internal EAC policies and precedent and may already have impaired the legitimate right to vote of many Americans. These concerns have been validated recently by the U.S. Court of Appeals for the D.C. Circuit, which has now issued an order temporarily halting and reversing Mr. Newby's action because of "irreparable harm" and the "public interest."²

We appreciate that Mr. Newby and Mr. Tatum provided a briefing to our staff on August 1, 2016. However, our staff was troubled to learn the following information at the briefing:

¹ Letter from Ranking Member Elijah E. Cummings, Ranking Member Robert A. Brady, and Assistant Democratic Leader James E. Clyburn to Election Assistance Commission Chairman Thomas Hicks (June 1, 2016).

² *League of Women Voters of the United States, et al v. Brian D. Newby, In His Capacity as the Executive Director of the United States Election Assistance Commission, et al*, No. 16-5196, (DC Cir. Sept. 9, 2016) (judgment).

The Honorable Thomas Hicks, Mr. Brian Newby, and Mr. Cliff Tatum
Page 2

- Mr. Newby conducted no written analysis regarding the impact of his unilateral decision to require proof of citizenship on the ability of eligible voters to register to vote. He conducted no cost-benefit analysis of the impact of his decision to compare the potential for voter fraud to the potential for eligible voter disenfranchisement. This is concerning given reports that in Kansas alone, state records show that, as early as April, at least 30,000 applicants had been denied registration due to lack of documents, and some believe the actual number could have been as high as 45,000.³
- Mr. Newby conceded that neither Alabama nor Georgia submitted any evidence that proof of citizenship requirements are necessary for those states to effectively administer their elections as required in the U.S. Supreme Court's ruling in *Arizona v. InterTribal Council of Arizona* and the Tenth Circuit Court of Appeals' decision in *Kobach v. EAC*. Kansas reportedly submitted a report of only one ineligible voter in a single county.
- Mr. Newby, the Executive Director of the nation's top election administration agency, claimed that he had been unaware until recently that proof of citizenship laws could have a disproportionate impact on people of color. This is especially disturbing since it has been widely reported that these proof of citizenship laws unduly burden not only people of color, but young voters, women, the elderly, people with disabilities, low-income voters, and the homeless.⁴
- Mr. Newby was aware that in the past, EAC had denied similar requests by states to require proof of citizenship through the state instructions to the federal form. Mr. Newby was also aware that his unilateral decision would depart from that past precedent, but he claimed that he "needed to have a point of view" and did not want to "rubber stamp" past precedent.
- Mr. Newby knew prior to his action that Commissioner Hicks, the Vice Chairman of the EAC at the time, believed that the requests regarding proof-of-citizenship constituted a question of policy and therefore could not be handled by the Executive Director unilaterally.
- Disregarding past precedent, EAC policies, and his conversation with the then-Vice Chairman, Mr. Newby decided to act alone rather than requesting a vote of the EAC or seeking public comment.

³ *The Voter Support Agency Accused of Suppressing Votes*, New York Times (Apr. 8, 2016).

⁴ See, e.g., *Citizens Without Proof: A Survey of Americans' Possession of Documentary Proof of Citizenship and Photo Identification*, Brennan Center for Justice, New York University School of Law (Nov. 28, 2006); Wendy R. Weiser, Keesha Gaskins, and Sundeep Iyer, "Citizens Without Proof" Stands Strong, Brennan Center for Justice, New York University School of Law (Sept. 8, 2011); and Stuart Naifeh, *How Do Proof-of-Citizenship Laws Block Legitimate Voters?* Demos (Aug. 25, 2014).

The Honorable Thomas Hicks, Mr. Brian Newby, and Mr. Cliff Tatum
Page 3

- Mr. Newby admitted that, at the time of the decision, he did not believe the action would violate the National Voter Registration Act (NVRA), but now he believes that it is unclear.

In seeking a better understanding of Mr. Newby's unilateral action, we requested specific documents and information. Unfortunately, EAC has withheld large categories of documents from Congress, claiming they are privileged or unable to be produced as a result of the court's protective order.

At the August 1 briefing, Mr. Tatum, EAC's General Counsel, committed to responding by the end of that week about whether EAC would produce redacted copies of documents over which EAC has claimed a privilege and would ask the Department of Justice to request that the court allow EAC to produce documents covered by the protective order.

Despite a follow-up email on August 12, 2016, Mr. Tatum has not provided a response to date.

Raising additional concerns, we also learned that on November 8, 2012, Mr. Newby wrote on his own blog, "No election administrator has been more in favor of closing the EAC than me."⁵ On January 28, 2014, Mr. Newby wrote on the same blog, "the EAC is now a 'was'."⁶

Given these troubling findings, we request that you produce all documents withheld for attorney-client or deliberative process privileges, with the privileged portions redacted. We also request that you arrange for staff to hold meetings with each EAC Commissioner to learn more about their conversations with Mr. Newby and about his unilateral decision.

Finally, given the new information Mr. Newby has obtained about the disproportionate impact of his decision on people of color, his lack of analysis regarding the impact on eligible voters' ability to vote, and his lack of clarity as to whether his decision undermines the NVRA, we request that Mr. Newby rescind his unilateral decision and reconsider it in a manner consistent with the U.S. Constitution, the NVRA, past EAC precedent, and current EAC policies and procedures.

We request a response by October 6, 2016. Please contact Karen Kudelko of Ranking Member Cummings' staff at (202) 225-5051, Khalil Abboud with Ranking Member Brady's staff at (202) 225-2061, or Amy Miller Pfeiffer with Assistant Democratic Leader Clyburn's staff at (202) 226-3210 with any questions.

Thank you for your consideration of this request.

⁵ Brian Newby, Election Diary, *We've Got to Fix This* (Nov. 8, 2012) (online at electiondiary-briandnewby.blogspot.com/2012/11/weve-got-to-fix-this.html).

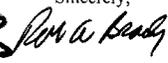
⁶ Brian Newby, Election Diary, *Chronicles of Yarnia, Part One* (Jan. 28, 2014) (online at http://electiondiary-briandnewby.blogspot.com/2014_01_01_archive.html).

The Honorable Thomas Hicks, Mr. Brian Newby, and Mr. Cliff Tatum
Page 4

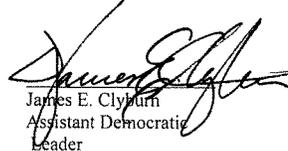
Sincerely,



Elijah Cummings
Ranking Member
Committee on Oversight
and Government Reform



Robert A. Brady
Ranking Member
Committee on House
Administration



James E. Clyburn
Assistant Democratic
Leader

States Ask Feds for Cybersecurity Scans Following Election Hacking Threats

BY: Nafeesa Syeed, Bloomberg News | September 19, 2016

(TNS) — A spate of hacking attacks has put U.S. states on edge ahead of November's presidential vote as election officials rush to plug cybersecurity gaps with help from the federal government.

Nine states have asked for "cyber hygiene" scans in which the Department of Homeland Security looks for vulnerabilities in election authorities' networks that are connected to the internet, according to a DHS official who asked not to be identified because the information isn't public. With less than two months before the election, DHS wants more states to sign up.

The threat — primarily from foreign hackers or intelligence agencies — affects states that are reliably Democratic or Republican as well as key battlegrounds including Pennsylvania and Ohio, officials and cybersecurity experts said. While hackers may not be able to change the actual outcome from afar, they could sow doubts by manipulating voter registration websites, voter databases and systems used to track results on election night.

"We're certainly on high alert," said Dean Logan, the registrar-recorder and county clerk in Los Angeles County, the nation's biggest electoral district. "Across the whole network of services and online applications for the county there are frequent indications of attempts to get into those systems."

Most states use voting equipment that can generate a paper record, allowing for audits or recounts if the result is close or tampering is suspected. Among the exceptions is Pennsylvania, which both Hillary Clinton and Donald Trump are targeting as a priority.

The electronic voting machines in 50 of Pennsylvania's 67 counties leave no paper trail, according to Verified Voting, a California-based nonprofit that monitors voting methods. Many of those counties use touch-screen machines, which are especially vulnerable, according to Andrew Appel, a computer science professor at Princeton University who stores in a warehouse the old voting machines that his research teams have hacked over the past dozen years.

Though the touch-screen machines aren't connected to the internet — where hackers can do damage from around the world — someone with physical access to the devices could employ techniques such as inserting a cartridge carrying malware that could reprogram their software, he said. Similar machines are used in Louisiana, New Jersey, South Carolina, Tennessee and Texas.

"There's no way to know that they have been hacked," Appel said. "And there's no way to recover what the vote should have been, and there's no way to know that the votes may be wrong."

Marian Schneider, Pennsylvania's deputy secretary for elections and administration, said her state is taking advantage of DHS's offer to scan computer systems and is considering hiring a contractor to bolster cybersecurity.

"We're going to be making sure that there are no exploitable vulnerabilities in our systems," said Schneider, whose agency oversees everything from state voter registration databases to aggregating local election results.

In a recent simulation, Symantec Corp. said its workers were able to easily hack into an electronic voting machine. It was possible to switch votes as well as change the volume of data, said Samir Kapuria, senior vice president and general manager of Symantec's cybersecurity group.

"It was pretty vulnerable to multiple attacks both physically as well as when that information got transmitted upstream for the tabulation systems," Kapuria said, without providing the machine's maker or saying where it is used. Symantec is working with the manufacturer to make improvements, he added.

6/20/2017

www.governing.com/templates/gov_print_article?id=394005991

DHS's major concern isn't necessarily a hacker changing ballots on Election Day, but an actor stirring up enough confusion in the "election infrastructure" as to undermine public confidence in the vote, according to the agency's official.

In an Aug. 1 speech in Columbus, Ohio, Republican presidential nominee Donald Trump said that he's "afraid the election is going to be rigged, I have to be honest," and he said cheating would be the reason if he loses Pennsylvania.

The DHS "cyber hygiene" assessments are quick tests that let states know of holes they should urgently fix. The department also is in talks with some states to do on-site visits to scan election authorities' internal networks that aren't linked to the internet. But with less than two months to go, few states will receive such a deep dive. States have told the feds it would be disruptive at this point to examine individual voting machines, so DHS will have to save those tests for after the election.

Concern about election tampering rose after hackers attacked servers at the Democratic National Committee and related organizations, taking internal emails and data that were made public on the WikiLeaks website. The revelations prompted DNC Chairwoman Debbie Wasserman Schultz to resign days before Clinton was formally named the party's nominee.

The FBI has "high confidence" recent attacks were orchestrated by Russia, according to a person familiar with the agency's probe. President Vladimir Putin has rejected the accusations.

FBI Director James Comey has said his agency is working "very hard to understand" whether a foreign government is hacking U.S. systems in order to influence elections or other national affairs.

Working against foreign hackers is the sheer complexity of the decentralized U.S. electoral system, which has about 9,000 separate jurisdictions where citizens go to vote.

"The beauty of the American voting system is that it's diverse among the 50 states and it's clunky as heck," Comey said Sept. 8 at a conference in Washington. "It is hard for an actor to reach our voting processes."

Besides the voting machines, hackers looking to cause chaos on Election Day could alter voter registration records and electronic poll-books, used to verify voters' identities at precincts. Local jurisdictions also worry about hackers tampering with websites that tell people where to vote or provide other information about the voting process.

During California's June presidential primary, a number of voters in Riverside County found that their party affiliations had been changed, according to District Attorney Michael Hestrin. He said it appeared hackers accessed voter-registration data. In some cases, voters even found their race, address and birth date changed, Riverside County Republican Party Chairman Scott Mann said. Others didn't find themselves in poll-books, Mann said.

Meddling with systems that tabulate and report the votes on election night — whether state election boards or media organizations — is another potential entry point for those wanting to cause mischief and undercut public confidence.

Ohio Secretary of State Jon Husted, a two-term Republican, said the state's elections systems have been modernized with cybersecurity upgrades in recent years, and "there's been nothing that's occurred that's given us any alarm."

Even before the FBI warned state officials last month to improve election security, Husted said his office consulted with the agency and with the state's cybersecurity experts. It even had the National Guard try to hack into Ohio's election system to identify any vulnerabilities.

"Everything that we should be doing, we were already doing before these alerts came about," Husted said in an interview in Columbus. "If you waited until the FBI called two weeks ago, then you were late."

(Mark Niquette, Chris Strohm and Jordan Robertson contributed to this report.)

©2016 Bloomberg News. Visit Bloomberg News at www.bloomberg.com. Distributed by Tribune Content

This article was printed from: <http://www.govtech.com/security/States-Ask-Feds-Cybersecurity-Scans-Following-Election-Hacking-Threats.html>



U. S. ELECTION ASSISTANCE COMMISSION

Voting System Testing and Certification Program
 1335 East West Highway, Suite 4300
 Silver Spring, MD 20910

Checklist for Securing Voter Registration Data

The Help America Vote Act (HAVA) requires that each State, acting through the chief State election official, shall implement, in a uniform and nondiscriminatory manner, a single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the State level that contains the name and registration information of every legally registered voter in the State and assigns a unique identifier to each legally registered voter in the State...

State requirements for registration differ greatly, but every State maintains personally identifiable information associated with the voter's name to determine eligibility and precinct information. Due to the sensitive nature of this personal information, there is a natural concern on what security protocol has been used to secure the data.

This list is intended to provide election officials information on best practices to protect their voter registration data. State and local election officials have already implemented many of these items. Election officials may use it to provide assurance to members of the public who may question the security measures that have been implemented in their State.

- Access Control** – only authorized personnel should have access to the voter registration database. Each person with authorization to the database should only have access to the data and information necessary for them to perform their job duties.
- Auditability** – the database should have sufficient logging capabilities, including who has made modifications, the nature of the modifications, the authority to make those modifications, and to determine if there has been any unauthorized or inappropriate activity.
- Detection** – use an intrusion detection system and monitor the incoming and outgoing traffic for signs of irregularities, such as multiple log-in attempts, above average traffic, large amounts of data being transmitted, etc. If detected have a response and mitigation plan in place.
- Data Backups** – the database should be backed up routinely. If any unexpected modifications to the data were to occur, the database could be restored to the last known state prior to the unexpected modifications. The ability to perform backups and restores should be tested and validated.

- ❑ **Data Suppression** – any data provided to outside sources is suppressed to only contain the data necessary for that entity to perform its legally authorized functions. For example, if an entity wants to obtain a copy of the data files to determine where specific voters live for GOTV campaigns, it does not need data field containing ID numbers and therefore, the additional information should not be provided.
- ❑ **Encryption** – encryption should be used throughout, including but not limited to encrypting the database, server, backups, any files used for distribution, all data transmission and communication.
- ❑ **Firewalls** – implementation of the proper use of network firewalls for the environment in use. Unauthorized access (or attempts to access) to the data should be detected, prevented, reported and escalated.
- ❑ **Remote Access Control** – only allow remote access through secure networks, such as Virtual Private Networks (VPN).
- ❑ **System Interconnection** – do not connect the voter registration database to any other information system that is not required for its use. When the voter registration system is required to be interconnected with another information system make sure the necessary security controls are in place for each system individually, as well as the communication channel between the systems.
- ❑ **Documentation** – when data is obtained from an authorized entity, make sure to maintain documentation on who was provided the information, for what purpose, and what information was contained within the data set. If data is inappropriately distributed, it will be easier to determine the source distribution.

Conclusion: The security of voter registration data along with providing the assurance to the public that the data has been protected is of the utmost importance to every election official. Any database containing personal information should be protected with strategic layers of physical and technological security. Election officials may use this list as a baseline to assess the current security protocol surrounding the voter registration database as well as a reference to guide the public on what has already been implemented to protect their voter registration data and the integrity of their vote.

Resources: For additional technical resources, reference the following documents.

- [National Institute of Standards and Technology \(NIST\) Cybersecurity Framework \(CSF\)](#)
- [NIST Special Publication 800-30](#)
- [NIST Special Publication 800-39](#)
- [International Organization for Standardization \(ISO\) 31000:2009](#)
- [ISO/IEC 27005:2011](#)

Congress of the United States
Washington, DC 20515

August 30, 2016

The Honorable James Comey
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue NW
Washington, D.C. 20530

Dear Mr. Director:

Based on multiple press reports, it appears that the Federal Bureau of Investigation (FBI) is investigating whether Russia executed cyber attacks against the Democratic National Committee (DNC) and the Democratic Congressional Campaign Committee (DCCC) that resulted in the illegal hacking of a wide range of emails and other documents.¹

We are writing to request that the FBI assess whether connections between Trump campaign officials and Russian interests may have contributed to these attacks in order to interfere with the U.S. presidential election.

Serious questions have been raised about overt and covert actions by Trump campaign officials on behalf of Russian interests. It is critical for the American public to know whether those actions may have directly caused or indirectly motivated attacks against Democratic institutions and our fundamental election process.

On July 22, 2016, just days before the Democratic convention, approximately 20,000 pages of illegally hacked documents were leaked by WikiLeaks in an apparent attempt to influence the U.S. presidential election in favor of Donald Trump.² According to one press report:

The FBI suspects that Russian government hackers breached the networks of the Democratic National Committee and stole emails that were posted to the anti-secrecy site

¹ See, e.g., *FBI Investigating Whether Russians Hacked Democratic Party's Emails to Help Donald Trump*, Los Angeles Times (July 25, 2016) (online at www.latimes.com/nation/la-na-pol-fbi-hack-dnc-russia-20160725-snap-story.html). See also *Growing Evidence Suggests Recent Hacks the Work of Russian-Backed Cyber Militias*, Fox News (Aug. 20, 2016) (online at www.foxnews.com/politics/2016/08/20/growing-evidence-suggest-recent-hacks-work-russian-backed-cyber-militias.html).

² *WikiLeaks Releases Thousands of Documents About Clinton and Internal Deliberations*, Washington Post (July 22, 2016) (online at www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/).

The Honorable James Comey
Page 2

WikiLeaks on Friday. It's an operation that several U.S. officials now suspect was a deliberate attempt to influence the presidential election in favor of Donald Trump, according to five individuals familiar with the investigation of the breach.³

Donald Trump has repeatedly praised Russian President Vladimir Putin, stating that "he's doing a great job,"⁴ "I'd get along very well with Vladimir Putin,"⁵ and "It is always a great honor to be so nicely complimented by a man so highly respected."⁶ Donald Trump's business interests in Russia have also been widely reported.⁷

Donald Trump has proposed shocking policy positions that would greatly benefit Russia, including breaking from longstanding U.S. commitments to our NATO allies to combat Russian aggression⁸ and weakening sanctions and recognizing Russia's annexation of Crimea.⁹

Of direct concern, however, are Donald Trump's comments encouraging Russian hacking and his top aides' previously undisclosed connections to Russian officials and interests.

On July 27, 2016—the third day of the Democratic convention—Donald Trump urged Russia to hack Secretary Hillary Clinton's emails.¹⁰

³ *FBI Suspects Russia Hacked DNC; U.S. Officials Say it Was to Elect Donald Trump*, Daily Beast (July 25, 2016) (online at www.thedailybeast.com/articles/2016/07/25/fbi-suspects-russia-hacked-dnc-u-s-officials-say-it-was-to-elect-donald-trump.html).

⁴ *Larry King Live*, CNN (Oct. 15, 2007) (online at www.cnn.com/TRANSCRIPTS/0710/15/lkl.01.html).

⁵ *Donald Trump: "I'd Get Along Very Well With Vladimir Putin"*, CBS News (July 30, 2015) (online at www.cbsnews.com/news/donald-trump-id-get-along-very-well-with-vladimir-putin/).

⁶ *Trump Says "Great Honor" to Get Compliments from "Highly Respected" Putin*, ABC News (Dec. 17, 2015) (online at <http://abcnews.go.com/Politics/trump-great-honor-compliments-highly-respected-putin/story?id=35829618>).

⁷ *Inside Donald Trump's Financial Ties to Russia and His Unusual Flattery of Vladimir Putin*, Washington Post (June 17, 2016) (online at www.washingtonpost.com/politics/inside-trumps-financial-ties-to-russia-and-his-unusual-flattery-of-vladimir-putin/2016/06/17/dbdcaac8-31a6-11e6-8ff7-7b6c1998b7a0_story.html?postshare=1821472042965377&tid=ss_mail).

⁸ *Trump Takes Heat from NATO Officials for Interview Comments*, Fox News (July 21, 2016) (online at www.foxnews.com/politics/2016/07/21/trump-takes-heat-from-nato-officials-for-interview-comments.html).

⁹ *This Week with George Stephanopoulos*, ABC News (July 31, 2016) (online at <http://abcnews.go.com/Politics/week-transcript-donald-trump-vice-president-joe-biden/story?id=41020870>).

¹⁰ *Trump Urges Russia to Hack Clinton's Email*, Politico (July 27, 2016) (online at www.politico.com/story/2016/07/trump-putin-no-relationship-226282).

The Honorable James Comey
Page 3

Less than two weeks later, on August 8, 2016, Roger Stone, a Donald Trump confidante, revealed that he has communicated with WikiLeaks founder Julian Assange about the upcoming release of additional illegally-hacked Democratic documents. Mr. Stone made these statements during a Republican campaign event while answering a question about a potential "October surprise."¹¹

It is unclear whether U.S. law enforcement authorities have interviewed Mr. Stone about his communications with Mr. Assange or about his knowledge of how WikiLeaks obtained the illegally-hacked documents.

In addition, on July 7, 2016, one of Donald Trump's foreign policy advisers, Carter Page, traveled to Moscow to give a speech that was harshly critical of the United States and its "hypocritical focus on ideas such as democratization, inequality, corruption and regime change."¹² Mr. Page had touted his extensive dealings with Russian energy giant Gazprom, claiming that he had been an adviser "on key transactions for Gazprom."¹³ After Donald Trump named Mr. Page as his foreign policy adviser in March, Mr. Page explained that "his business has suffered directly from the U.S. economic sanctions imposed after Russia's escalating involvement in the Ukraine."¹⁴

Mr. Page appears to enjoy high-level access to Russian officials that are currently under sanctions imposed by the United States government. According to one press report:

After the Obama administration added Rosneft Chairman Igor Sechin to its sanctions list in 2014, limiting Sechin's ability to travel to the United States or do business with U.S. firms, Page praised the former deputy prime minister, considered one of Putin's closest allies over the past 25 years. "Sechin has done more to advance U.S.-Russian relations than any individual in or out of government from either side of the Atlantic over the past decade," Page wrote.¹⁵

¹¹ *Trump Ally Claims He "Communicated With" WikiLeaks Founder*, Washington Examiner (Aug. 9, 2016) (online at www.washingtonexaminer.com/trump-ally-claims-he-communicated-with-wikileaks-founder/article/2598931).

¹² *Trump's Russia Adviser Criticizes U.S. for "Hypocritical Focus on Democratization,"* Washington Post (July 7, 2016) (online at www.washingtonpost.com/world/europe/trumps-russia-adviser-criticizes-us-for-hypocritical-focus-on-democratization/2016/07/07/804a3d60-4380-11e6-a76d-3550dba9226ac_story.html).

¹³ *Biography of Carter Page, CFA*, Global Energy Capital LLC (accessed Aug. 22, 2016) (online at www.globalenergycap.com/management/).

¹⁴ *Trump's New Russia Adviser Has Deep Ties to Kremlin's Gazprom*, Bloomberg (Mar. 30, 2016) (online at www.bloomberg.com/politics/articles/2016-03-30/trump-russia-adviser-carter-page-interview).

¹⁵ *Trump Adviser's Public Comments, Ties to Moscow Stir Unease in Both Parties*, Washington Post (Aug. 5, 2016) (online at www.washingtonpost.com/business/economy/trump-advisers-public-comments-ties-to-moscow-stir-unease-in-both-parties/2016/08/05/2e8722fa-5815-11e6-9aee-8075993d73a2_story.html).

The Honorable James Comey
Page 4

It is unclear whether U.S. law enforcement authorities have interviewed Mr. Page about whether he met with Mr. Sechin or other individuals on the U.S. sanctions list during his trip to Moscow or on other occasions.

Another top adviser to Donald Trump, Lt. Gen. Michael Flynn, traveled to Moscow in December 2015 and joined Vladimir Putin at the head table during a dinner honoring the Kremlin-backed media network RT. During the event, General Flynn gave a speech that was highly critical of the United States, stating, “The United States can’t sit there and say, ‘Russia, you’re bad.’”¹⁶ The following week, President Putin praised Donald Trump as “an outstanding and talented personality.”¹⁷ General Flynn declined to answer media inquiries about whether he traveled to Moscow on Donald Trump’s behalf.¹⁸

Most recently, Donald Trump’s campaign chairman, Paul Manafort, resigned after failing to disclose his role in assisting a pro-Russian party in Ukraine. Mr. Manafort reportedly had “wooded investments from oligarchs linked to Putin and advised the now-toppled pro-Russian Ukrainian president Viktor Yanukovich.”¹⁹ According to one press account:

Donald Trump’s campaign chairman helped a pro-Russian governing party in Ukraine secretly route at least \$2.2 million in payments to two prominent Washington lobbying firms in 2012, and did so in a way that effectively obscured the foreign political party’s efforts to influence U.S. policy. ... Under federal law, U.S. lobbyists must declare publicly if they represent foreign leaders or their political parties and provide detailed reports about their actions to the Justice Department. A violation is a felony and can result in up to five years in prison and a fine of up to \$250,000.²⁰

Rick Gates, a top strategist in Donald Trump’s campaign, reportedly worked with Mr. Manafort on this effort, “helping steer the advocacy work done by a pro-Yanukovich nonprofit,” including “downplaying the necessity of a congressional resolution meant to pressure the

¹⁶ *Trump Embraces Ex-Top Obama Intel Official*, Daily Beast (Mar. 9, 2016) (online at www.thedailybeast.com/articles/2016/03/09/donald-trump-embraces-top-obama-intel-official.html).

¹⁷ *Putin Praises “Bright and Talented” Trump*, CNN (Dec. 17, 2015) (online at www.cnn.com/2015/12/17/politics/russia-putin-trump/).

¹⁸ *Trump Embraces Ex-Top Obama Intel Official*, Daily Beast (Mar. 9, 2016) (online at www.thedailybeast.com/articles/2016/03/09/donald-trump-embraces-top-obama-intel-official.html).

¹⁹ *Trump Adviser’s Public Comments, Ties to Moscow Stir Unease in Both Parties*, Washington Post (Aug. 5, 2016) (online at www.washingtonpost.com/business/economy/trump-advisers-public-comments-ties-to-moscow-stir-unease-in-both-parties/2016/08/05/2e8722fa-5815-11e6-9aee-8075993d73a2_story.html).

²⁰ *Manafort Tied to Undisclosed Foreign Lobbying*, Associated Press (Aug. 17, 2016) (online at <http://bigstory.ap.org/article/c01989a47ee5421593ba1b301ec07813/ap-sources-manafort-tied-undisclosed-foreign-lobbying>).

The Honorable James Comey
Page 5

Ukrainian leader to release an imprisoned political rival.”²¹ Although Mr. Manafort has resigned from his position, it appears that Mr. Gates continues to be a top adviser to Mr. Trump.

It is unclear whether U.S. law enforcement authorities have interviewed Mr. Manafort or Mr. Page about their failure to disclose this information, but several prominent Members of Mr. Trump’s party have expressed grave concerns.

For example, Republican Adam Kinzinger of Illinois called for an investigation into Donald Trump’s “chief adviser, what his association with the Russians are.” More broadly, Rep. Kinzinger criticized “this affection in the campaign for Russia and Vladimir Putin,” and he questioned how and why a reference to Russian offensive weapons was mysteriously removed from the Republican Party’s platform, noting that “it just happened.”²²

Similarly, Eliot Cohen, who served as a counselor at the State Department under the George W. Bush Administration, warned: “Foreign governments sometimes express preferences about who should be elected; that’s already problematic. But to do something in the nature of dirty tricks would be a very, very serious problem.”²³

Finally, House Speaker Paul Ryan’s spokesman stated: “Russia is a global menace led by a devious thug. Putin should stay out of this election.”²⁴

We do not know if Donald Trump’s public statements or the connections of his campaign officials to Russian interests directly or indirectly led to the cyber attacks against Democratic party organizations, but there is widespread agreement that the United States should take all steps possible to prevent Russia from interfering in our electoral process and prosecute to the full extent of the law anyone involved in such a scheme.

²¹ *Id.*

²² *GOP Congressman Warns Trump: Russia Not an Ally*, CNN (Aug. 6, 2016) (online at www.cnn.com/videos/tv/2016/08/15/gop-congressman-rep-adam-kinzinger-reacts-to-trumps-isis-plan-the-lead.cnn); *Rep. Kinzinger Calls for Investigation Into Manafort-Russian Ties*, Politico (Aug. 6, 2016) (online at www.politico.com/story/2016/08/gop-rep-calls-for-investigation-into-manafort-russian-ties-227090). See also *Donald Trump Campaign Chairman Paul Manafort Resigns*, CNN (Aug. 20, 2016) (online at www.cnn.com/2016/08/19/politics/donald-trump-campaign-chairman-paul-manafort-resigns/index.html) (citing Rep. Sean Duffy of Wisconsin, stating, “I want to know what money he got from a pro-Russian organization in the Ukraine.”).

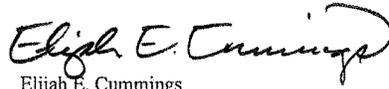
²³ *Trump Invites Russia to Meddle in the U.S. Presidential Race with Clinton’s Emails*, Washington Post (July 27, 2016) (online at www.washingtonpost.com/politics/trump-invites-russia-to-meddle-in-the-us-presidential-race-with-clintons-emails/2016/07/27/a85d799c-5414-11e6-b7de-dfe509430c39_story.html?tid=a_inl).

²⁴ *Speaker Paul Ryan Calls on “Global Menace” Russia to “Stay Out of This Election;” The Call Came After Donald Trump Encouraged Russian Hackers to Target Hillary Clinton*, CNN (July 27, 2016) (online at <http://time.com/4426783/paul-ryan-republicans-donald-trump-russia/>).

The Honorable James Comey
Page 6

Thank you for your consideration of this request.

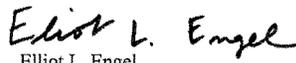
Sincerely,



Elijah E. Cummings
Ranking Member
Committee on Oversight and
Government Reform



John Conyers, Jr.
Ranking Member
Committee on the Judiciary



Elliot L. Engel
Ranking Member
Committee on Foreign Affairs



Bennie G. Thompson
Ranking Member
Committee on Homeland Security

cc: The Honorable Jason Chaffetz
The Honorable Bob Goodlatte
The Honorable Edward R. Royce
The Honorable Michael T. McCaul



September 26, 2016

**Open Letter from the Nation's Secretaries of State to Congress:
Let's Work Together to Share the Facts about Cybersecurity and Our Elections**

As Congress looks into national security concerns about cyber threats to our election, the nation's Secretaries of State who serve as chief state election officials are issuing this letter via the National Association of Secretaries of State (NASS). Our bipartisan message: States are on high alert and will continue to vigilantly monitor their election systems for ongoing cyber threats and vulnerabilities. Fortunately, we have an infrastructure in place that will enable election officials to deal with problems in both the short and long-run. Understanding some basic facts about our system is important.

Of course, with talk of "rigged" elections and Russian attacks, there is much cause for concern. Recent efforts to mine data from voter registration systems in at least two states serve as an important warning against international cyber threats. As our national security agencies work to address any attempts by nation-state adversaries to disrupt the presidential election and call its integrity into question, there are many questions to be asking, including what constitutes an appropriate response and how to prevent further intrusions.

As public officials at all levels of government collaborate on these issues, there are important ways in which we can work together:

1) LET'S MAKE SURE THE AMERICAN PUBLIC UNDERSTANDS THE BUILT-IN SAFEGUARDS IN OUR PROCESS

Election officials are working overtime to help the public understand the components of our election process and some of the built-in safeguards that exist. Elections are largely administered by states and localities. Voting systems are spread out in a highly-decentralized structure covering more than 9,000 election jurisdictions and hundreds of thousands of polling locations. Machines are standalone and do NOT connect to the Internet. There are multiple layers of physical and technical security surrounding our systems. U.S. Department of Homeland Security (DHS) Secretary Jeh Johnson and FBI Director James Comey have both publicly stated that our process makes it highly unlikely that hackers can hijack election outcomes, as there is no central point of entry and NO NATIONAL SYSTEM to be attacked. In fact, there is no evidence that ballot manipulation has ever occurred in the U.S. via cyberattack.

Election officials welcome questions about security, and there are a range of options for getting more involved in the process – including becoming a poll worker to witness the process first-hand!

2) LET'S WORK TOGETHER TO KEEP OUR ELECTIONS SECURE

Just as we must have contingency plans for floods and all kinds of natural phenomena, we must also be ready to deal with man-made threats. The risks posed by foreign government hackers, cyber criminals and everyday hacktivists are not new to election officials. States and localities



**National Association of Secretaries of State
Open Letter to Congress: Cybersecurity and Our Elections**

are committed to working with national security agencies and other federal partners, including the U.S. Election Assistance Commission (EAC) and the National Institute of Standards and Technology (NIST), to solicit input on threats and risk mitigation in our elections. States are already deploying numerous resources for this election cycle, including extensive testing for cyber threats described by the recent FBI alert, and best practices guidelines produced by the EAC. Additional steps may be taken based upon credible or specific threats that are identified in the run-up to Election Day. Secretaries of State are also part of a DHS Election Infrastructure Cybersecurity Working Group, created for sharing resources, best practices and technical advice.

To be clear: The equipment that people vote on is NOT connected to the Internet. Vote counting is NEVER done with systems connected to the Internet, and tabulation systems are not networked. Election systems must be physically secured when not in use, with public accuracy and performance testing that anyone can observe. Post-election audits can help to further guard against deliberate manipulation of the election, as well as unintentional software, hardware or programming issues. Again, there are no documented cases of flawed voting results linked to alleged cyber hacking.

3) LET'S NOT CONFUSE NON-VOTING SYSTEMS WITH OUR VOTING SYSTEMS

Election management and voter registration systems make the voting process more efficient and accessible, but they are not linked to vote casting or counting. While it is theoretically possible to disrupt an election via networked systems, their compromise will not affect election results. These systems have their own fail-safes and contingency solutions that would make it highly difficult to leverage them for changing outcomes. Poll books, printed records, back-ups and back-ups of back-ups all provide multiple layers of security around this part of the process. Plus, information collected through online voter registration systems typically does not flow directly into statewide registration databases. Instead, voter information is sent to each local registrar of voters for processing.

Most importantly, anyone who discovers an issue with their voter registration status when they show up at a polling place will still have options for casting a ballot. Every state has routine procedures for assisting voters whose names don't appear on the voter rolls. Adding names to rolls won't help, unless hackers also have an army of impersonators on the ground to help perpetrate their scheme, and voter impersonation has been documented as a rare occurrence. Both DHS and FBI officials have declared these scenarios to be highly unlikely, instead pointing to "sowing doubt or confusion" as worst-case outcomes, which election officials would be able to address. Voters can also check their voter registration status through www.Canivote.org.

4) LET'S SUPPORT INVESTMENT IN OUR VOTING PROCESS

It is no secret that elections are underfunded and under-resourced. The bipartisan Presidential Commission on Election Administration (PCEA) identified an "impending crisis in voting technology" as a key issue to address in its final 2014 report. There is no quick fix for this reality.



**National Association of Secretaries of State
Open Letter to Congress: Cybersecurity and Our Elections**

For that, we need a longer-term investment in our elections at all levels of government. Many states and localities want to replace or update their aging voting equipment, which is approaching its useful end of life. These systems were purchased by federal funding from the Help America Vote Act (HAVA) in the years following the contentious presidential election in 2000. In 2010, NASS produced a funding report noting that \$396 million in HAVA funding remains to be appropriated by Congress.

Let's explore how an investment in voting technology can benefit the security of our nation's election process for the long-term, including cyber security as it relates to the federal development of voluntary voting systems standards for testing and certification overseen by the U.S. EAC and NIST. Besides asking what the next generation of voting technology will look like and how it will be secured, we must also determine how it will be adequately funded. This includes any kind of training that will be necessary to prepare the mammoth force of dedicated election officials and volunteers who run our system.

5) LET'S NOT TAKE ANY ACTIONS THAT WOULD UNNECESSARILY DAMAGE PUBLIC CONFIDENCE IN OUR PROCESS

There is no single piece of legislation or simple bureaucratic solution that can address all of the complex cyber security issues facing election officials, political parties and campaigns. While NASS currently has no position on a critical infrastructure designation by DHS, it has been made clear by Secretary Johnson that it will not come with additional funding for states and localities, and details on how this designation would be applied to elections are unclear. Some of our members have raised questions about how it would be possible to maintain public confidence in our elections, which are built on transparency and public access, if they are intermingled with national security agencies that understandably depend upon secrecy in their function. Others have been vocal in their view that such a designation would undercut the constitutional role that states and localities play in our elections and complicate the ability of states to work together with federal partners to combat cyber threats.

In the short-term, our goal is to avoid distractions and work together with our federal partners to secure the systems that are in place for the November election. Long-term, a larger dialogue is needed to avoid actions that would interfere with – or simply be perceived as interfering with – public ownership of elections by local communities and the citizens who run them, or be seen as threatening transparency and trust in our imperfect, but time-tested system of participatory democracy. Our collective imperative must be to ensure that actions to protect our elections do not create undue alarm or mistrust that will threaten voters' confidence in the outcomes.

Be sure to talk to your state and local election officials if you have additional questions. As we head into high gear for Election Day, Secretaries of State are taking every precaution to deliver a voting process that is not only safe and secure, but also fair, accurate and accessible. Voters must have no doubt that their votes – and votes alone – will determine the next President of the United States this November.



September 28, 2016

The Honorable William Hurd, Chairman
 The Honorable Robin Kelly, Ranking Member
 Subcommittee on Information Technology
 U.S. House Committee on Oversight & Government Reform
 2157 Rayburn House Office Building
 Washington, DC 20515

RE: Hearing on “Cybersecurity: Ensuring the Integrity of the Ballot Box”

Dear Chairman Hurd and Ranking Member Kelly:

The Electronic Privacy Information Center (“EPIC”) is a public interest research center established more than 20 years ago to focus public attention on emerging privacy and civil liberties issues. EPIC has a long history of working to protect voter privacy and election integrity.¹ EPIC, Verified Voting, and Common Cause last month released *The Secret Ballot at Risk: Recommendations for Protecting Democracy*, a report highlighting the right to a secret ballot and how Internet voting threatens voter privacy.² We have submitted a copy of the report with this letter. Additionally, in April 2015, as the result of a Freedom of Information Act lawsuit,³ EPIC obtained a September 2011 report about online voting from the Department of Defense. The report, produced in response to EPIC’s July 2014 FOIA request,⁴ summarizes a pilot test of e-voting system. The report recommends several changes, including accessibility and user interface, but does little to address privacy and security concerns except for recommending “visible security features” to “give users greater confidence in the privacy and security of their ballots.” EPIC has also previously submitted comments and testified before the Election Assistance Commission.⁵

¹ Voting Privacy, EPIC, <https://epic.org/privacy/voting/>.

² Caitriona Fitzgerald et al., *The Secret Ballot at Risk: Recommendations for Protecting Democracy* (2016), <http://secretballotatrisk.org>.

³ EPIC v. Dep’t of Defense, EPIC, <https://epic.org/foia/dod/e-voting/>.

⁴ EPIC, FOIA Request to Dep’t of Defense (July 17, 2014), <https://epic.org/privacy/voting/EPIC-FVAP-FOIA-Request-071714.pdf>.

⁵ See EPIC Comments to Election Assistance Comm’n (May 5, 2008), available at https://epic.org/privacy/voting/2007vvsg_5508.pdf; see also EPIC Comments to Election Assistance Comm’n (April 24, 2008), available at https://epic.org/privacy/voting/eac_test4_24.pdf.

The Secret Ballot

The right to cast a secret ballot in a public election is a core value in the United States' system of self-governance. Secrecy and privacy in elections guard against coercion and are essential to integrity in the electoral process. Secrecy of the ballot is guaranteed in state constitutions and statutes nationwide. However, as states permit the marking and transmitting of marked ballots over the Internet, the right to a secret ballot is eroded and the integrity of our elections is put at risk.

Since its widespread adoption in 1896, the concept of the secret ballot has remained a cornerstone of our democratic process. In the 1992 case of *Burson v. Freeman*, the Supreme Court described voter privacy as a means of preventing voter fraud while protecting against undue coercion.⁶ Upholding a Tennessee statute that prohibited political candidates from campaigning within 100 feet of a polling place entrance, the Court stated:

[A]n examination of the history of election regulation in this country reveals a persistent battle against two evils: voter intimidation and election fraud. After an unsuccessful experiment with an unofficial ballot system, all 50 States, together with numerous other Western democracies, settled on the same solution: a secret ballot secured in part by a restricted zone around the voting compartments. We find that this widespread and timetested consensus demonstrates that some restricted zone is necessary in order to serve the States' compelling interests in preventing voter intimidation and election fraud.⁷

Because of the documented history of voter intimidation, coercion, and fraud associated with third party knowledge of how individual voters cast their ballots, it is important not to underestimate the importance of voter privacy. No community is immune to the effects of voter manipulation, but some communities are more vulnerable than others—for example minorities, new citizens, or the poor. Our need for privacy protections is just as strong today as it was when the secret ballot was adopted.

Federal and state courts and legislatures have historically taken measures to protect the right of voters to vote their conscience without fear of retaliation.⁸ Our findings in *The Secret Ballot at Risk: Recommendations for Protecting Democracy* showed that 44 states have a constitutional provision guaranteeing that secrecy in voting shall be preserved.⁹ Some states, such as Alabama, provide an individual right to a secret ballot.¹⁰ Others, such as Delaware, require the state legislature to prescribe laws protecting ballot secrecy.¹¹ The six states (and DC)

⁶ *Burson v. Freeman*, 504 U.S. 191 (1992).

⁷ *Id.* at 206.

⁸ *See id.*

⁹ AK, AL, AR, AZ, CA, CO, CT, DE, FL, GA, HI, IA, ID, IL, IN, KS, KY, LA, MA, MD, ME, MI, MN, MO, MS, MT, NC, ND, NE, NM, NV, NY, OH, PA, SC, SD, TN, TX, UT, VA, WA, WI, WV, WY.

¹⁰ *See e.g.* Ala. Const. Art. VIII, § 177, as amended by Ala. Const. Amend. No. 865.

¹¹ *See e.g.* Del. Const. art. 5 § 1.

that do not have a constitutional provision regarding ballot secrecy have statutory provisions referencing secrecy in voting.¹²

Despite the strong recognition of the importance of the secret ballot in state constitutions and statutes, state governments are experimenting with Internet voting in public elections. Our state survey found that 32 states and D.C. offer Internet voting to at least some voters, typically military and overseas voters.¹³ In Alaska, all absentee voters can vote via the Internet. In Utah, voters with disabilities are also allowed to use the system. Of the 32 states and D.C. that offer some form of Internet voting, voters in 28 of those states and D.C. are explicitly required by state elections officials to sign a waiver of their right to a secret ballot in order to vote over the Internet. In the five other states, voters are permitted to cast ballots via the Internet with no warning from elections officials that their ballot may not remain secret.¹⁴

Internet voting will erode voter privacy and threaten election integrity. We need look no further than the warning all Alaska voters receive if they use the online voting system to cast their absentee ballots. Alaska acknowledges that the system is insecure and may not work, warning voters that “[w]hen returning the ballot through the secure online delivery system, your [sic] are voluntarily waving [sic] your right to a secret ballot and are assuming the risk that a faulty transmission may occur.”¹⁵ A similar warning on a physical polling place voting system would be considered unacceptable.

Recommendations on Voting and Privacy

1. Ballot secrecy and voter privacy should be the terms used to describe privacy within the context of voting technology standards as well guidelines related to certification and testing.
2. Ballot secrecy and voter privacy must be core values within the context of voting technology standards and testing and certification of voting systems.
3. Full sections on voter privacy should be included in each of the standards sections that address system operation.
4. Implement fail - safe approaches to ensure that when voting systems fail or malfunction they do so in a way that protects ballot secrecy, accuracy of the votes recorded, retained, and reported in final election results.
5. Internet voting should not be implemented in any public election.

¹² DC, NH, NJ, OK, OR, RI, VT.

¹³ AK, AL, AZ, CA, CO, DC, DE, FL, HI, IA, ID, IN, KS, LA, MA, ME, MO, MS, MT, NC, ND, NE, NJ, NM, NV, OK, OR, RI, SC, TX, UT, WA, and WV all offer some form of Internet voting.

¹⁴ Caitriona Fitzgerald et al., *The Secret Ballot at Risk: Recommendations for Protecting Democracy* 7-8 (2016), <http://secretballotatrisk.org>.

¹⁵ State of Alaska Division of Elections, *Absentee Voting by Electronic Transmission*, http://www.elections.alaska.gov/vi_bb_by_fax.php.

We look forward to working with you to ensure that voter privacy is protected in this election and elections to come.

Sincerely,

Marc Rotenberg

Marc Rotenberg
EPIC President

Caitriona Fitzgerald

Caitriona Fitzgerald
EPIC State Policy Coordinator

