AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

ELECTION SECURITY: VOTING TECHNOLOGY VULNERABILITIES

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

OF THE

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

JUNE 25, 2019

Serial No. 116–31

Printed for the use of the Committee on Science, Space, and Technology



Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
36–795PDF WASHINGTON : 2020

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. EDDIE BERNICE JOHNSON, Texas, *Chairwoman*

ZOE LOFGREN, California
DANIEL LIPINSKI, Illinois
SUZANNE BONAMICI, Oregon
AMI BERA, California,
Vice Chair
CONOR LAMB, Pennsylvania
LIZZIE FLETCHER, Texas
HALEY STEVENS, Michigan
KENDRA HORN, Oklahoma
MIKIE SHERRILL, New Jersey
BRAD SHERMAN, California
STEVE COHEN, Tennessee
JERRY MCNERNEY, California
ED PERLMUTTER, Colorado
PAUL TONKO, New York
BILL FOSTER, Illinois
DON BEYER, Virginia
CHARLIE CRIST, Florida
SEAN CASTEN, Illinois
KATIE HILL, California
BEN MCADAMS, Utah
JENNIFER WEXTON, Virginia

FRANK D. LUCAS, Oklahoma,
Ranking Member
MO BROOKS, Alabama
BILL POSEY, Florida
RANDY WEBER, Texas
BRIAN BABIN, Texas
ANDY BIGGS, Arizona
ROGER MARSHALL, Kansas
RALPH NORMAN, South Carolina
MICHAEL CLOUD, Texas
TROY BALDERSON, Ohio
PETE OLSON, Texas
ANTHONY GONZALEZ, Ohio
MICHAEL WALTZ, Florida
JIM BAIRD, Indiana
JAIME HERRERA BEUTLER, Washington
JENNIFFER GONZALEZ-COLÓN, Puerto Rico
VACANCY

SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT

HON. MIKIE SHERRILL, New Jersey, *Chairwoman*

SUZANNE BONAMICI, Oregon
STEVE COHEN, Tennessee
DON BEYER, Virginia
JENNIFER WEXTON, Virginia

RALPH NORMAN, South Carolina, *Ranking Member*
ANDY BIGGS, Arizona
MICHAEL WALTZ, Florida

SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

HON. HALEY STEVENS, Michigan, *Chairwoman*

DANIEL LIPINSKI, Illinois
MIKIE SHERRILL, New Jersey
BRAD SHERMAN, California
PAUL TONKO, New York
BEN MCADAMS, Utah
STEVE COHEN, Tennessee
BILL FOSTER, Illinois

JIM BAIRD, Indiana, *Ranking Member*
ROGER MARSHALL, Kansas
TROY BALDERSON, Ohio
ANTHONY GONZALEZ, Ohio
JAIME HERRERA BEUTLER, Washington

C O N T E N T S

June 25, 2019

Page

Hearing Charter 2

Opening Statements

Statement by Representative Mikie Sherrill, Chairwoman, Subcommittee on Investigations and Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives 9
Written Statement 10

Statement by Representative Ralph Norman, Ranking Member, Subcommittee on Investigations and Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives 11
Written Statement 12

Statement by Representative Haley Stevens, Chairwoman, Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives 13
Written Statement 14

Statement by Representative Jim Baird, Ranking Member, Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives 15
Written Statement 16

Written statement by Representative Eddie Bernice Johnson, Chairwoman, Committee on Science, Space, and Technology, U.S. House of Representatives 17

Written statement by Representative Frank Lucas, Ranking Member, Committee on Science, Space, and Technology, U.S. House of Representatives 18

Witnesses:

Dr. Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology
Oral Statement 20
Written Statement 22

Mr. Neal Kelley, Registrar of Voters, Orange County, California
Oral Statement 28
Written Statement 30

Dr. Latanya Sweeney, Professor of Government and Technology in Residence, Department of Government, Harvard University, Institute of Quantitative Social Science
Oral Statement 77
Written Statement 79

Mr. Paul Ziriax, Secretary, Oklahoma State Election Board
Oral Statement 84
Written Statement 86

Dr. Josh Benaloh, Senior Cryptographer, Microsoft Research
Oral Statement 99
Written Statement 101

Discussion 113

Page

Appendix I: Answers to Post-Hearing Questions

Dr. Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology 136
Mr. Neal Kelley, Registrar of Voters, Orange County, California 138
Dr. Josh Benaloh, Senior Cryptographer, Microsoft Research 140

Appendix II: Additional Material for the Record

Documents submitted Representative Mikie Sherrill, Chairwoman, Subcommittee on Investigations and Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives 146
Document submitted by Rep. Sean Casten, Committee on Science, Space, and Technology, U.S. House of Representatives 176

ELECTION SECURITY: VOTING TECHNOLOGY VULNERABILITIES

TUESDAY, JUNE 25, 2019

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT,
JOINT WITH THE SUBCOMMITTEE ON RESEARCH
AND TECHNOLOGY,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittees met, pursuant to notice, at 2:58 p.m., in room 2318 of the Rayburn House Office Building, Hon. Mikie Sherrill [Chairwoman of the Subcommittee on Investigations and Oversight] presiding.

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

HEARING CHARTER

Election Security: Voting Technology Vulnerabilities
Tuesday, June 25, 2019
2:00 p.m.
2318 Rayburn House Office Building

PURPOSE

The purpose of the hearing is to review the security of US election system technologies, such as e-poll books, voter registration systems, and voting machines, and the maintenance and operations activities that support them. The Subcommittees will discuss research and other activities being carried out under the Help America Vote Act (HAVA), which directed the National Institute of Standards and Technology (NIST) to develop voluntary voting systems guidelines in collaboration with the Election Assistance Commission (EAC). The Subcommittees will also explore policy strategies for protecting the full technology enterprise associated with election systems and recommendations from the 2018 National Academies report, *Securing the Vote: Protecting American Democracy*.

WITNESSES

- **Dr. Charles H. Romine**, Director, Information Technology Laboratory, National Institute of Standards and Technology
- **Mr. Neal Kelley**, Registrar of Voters, Orange County, California
- **Dr. Latanya Sweeney**, Professor of Government and Technology in Residence, Department of Government, Harvard University, Institute for Quantitative Social Science
- **Mr. Paul Ziriax,** Secretary, Oklahoma State Election Board
- **Dr. Josh Benaloh**, Senior Cryptographer, Microsoft Research

KEY QUESTIONS

- What are the technology components associated with conducting a secure election?
- What types of voting technology vulnerabilities were seen during the 2016 and 2018 election cycles?
- What are the roles of NIST and other science agencies in developing technologies and best practices for secure elections?
- What are some of the barriers that election officials face as they seek to enhance the security of their systems?
- Are legislative changes needed to adapt existing programs to modern technology issues?

BACKGROUND

Help America Vote Act (HAVA 2002) and Voluntary Voting System Guidelines (VVSG)

In October 2002, Congress passed the Help America Vote Act,[1] which (among other things) created the US Election Assistance Commission and authorized election-related activities at NIST.[2] Under HAVA, NIST carries out research to inform the development of the voluntary voting systems guidelines to be recommended to the EAC. This research includes security of computers used in voting systems, methods to detect and prevent fraud, protection of voter privacy, the role of human factors in the design and application of voting systems, and remote access voting.

HAVA also established the Technical Guidelines Development Committee (TGDC).[3] TGDC is the forum where voluntary voting system guidelines are developed, with NIST serving as the technical and administrative lead. The other members of TGDC include representatives of the EAC, representatives of the National Association of State Election directors (NASED), and outside experts.[4] The purpose of TGDC[5] is to develop voluntary voting system guidelines which states and counties in the U.S. can use to enhance the security, functionality, usability, accessibility, auditability, privacy etc. of their election systems.

The EAC Commissioners then vote to recognize the recommendations that TGDC promulgates. EAC also provides technical assistance and grants to states that support implementation of election system improvements according to TGDC guidelines. For example, in March 2018, the EAC awarded a grant to the New Jersey Secretary of State that would be used in part to implement secure Automatic Voter Registration at the NJ Motor Vehicle Commission and to pilot voting systems with a voter verified paper audit trail.[6]

HAVA 2002 does not establish any compulsory voting system security requirements for states; the Constitution grants states wide latitude in how to administer elections.[7] Any compulsory federal requirements would likely be issued by the Department of Homeland Security.

In 2004 NIST and the EAC released their first set of election administration protocols., the Voluntary Voting System Guidelines 1.0.[8] In March 2015, NIST and the EAC released an update, VVSG 1.1.[9] States have discretion whether to adopt some of all of the VVSG recommendations. As of 2019, 12 states require full federal certification of their election systems under VVSG.[10] Eight states have no federal testing or certification requirements.[11]

---

[1] Public Law 107–252
[2] https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/
[3] https://www.nist.gov/itl/voting
[4] https://www.eac.gov/about/tgdc-roster/
[5] https://www.eac.gov/assets/1/6/TGDC2019Charter.pdf
[6] https://www.eac.gov/payments-and-grants/hava-funds-state-chart-view/
[7] https://www.whitehouse.gov/about-the-white-house/elections-voting/
[8] https://www.eac.gov/assets/1/28/VVSG.1.0_Volume_1.PDF
[9] https://www.eac.gov/assets/1/28/VVSG.1.1.VOL.1.FINAL1.pdf
[10] DE, GA, ID, LA, NC, ND, OH, SC, SD, WA, WV, WY
[11] http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx

On February 15, 2019, the EAC Commissioners voted unanimously to publish a new VVSG promulgated by NIST, VVSG 2.0. The comment period closed on May 29, 2019. NIST is working now to resolve outstanding questions from the EAC and stakeholder process.

National Science Foundation Research

Another element of the U.S. election system within the Committee's purview is relevant research at NSF. As part of its own broad science mission, the National Science Foundation (NSF) carries out fundamental computer science research activities with relevance to election technology and social science research with relevance to voter interface with elections technology.

Technology Elements of the Voting System

Before The Vote

Voting registration portals/interfaces. There are more than 10,000 election jurisdictions in the United States. Depending on the jurisdiction, voters can register in person at election offices, at Departments of Motor Vehicles, or other public agencies.[12] Thirty-seven states and the District of Columbia allow for online voter registration, which can be conducted through state election board websites or within another public agencies' websites. Fifteen states allow same-day voter registration and 9 states and DC have automatic voter registration, where voters must "opt-out" when they interact with a government agency for another purpose (e.g. the DMV).[13]

Voter registration databases (VRDs). HAVA 2002 requires states to create a "single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the State level[14]" where voter registration data is stored. States use a variety of software products, with varying levels of cybersecurity controls, for the database platforms that aggregate and store this information. VRDs are then used to populate poll books.

Location election websites. Voters frequently use local and state election websites to seek information about where to cast their vote. Many jurisdictions' websites will allow voters to input their home address in order to be matched with their polling place.

Poll books. Poll books are the resource that poll workers use on election day to verify voters are who they say they are, and that they are eligible to vote in that location.[15] A transition from paper to "e-poll books" on computers or tablets has been underway for several years. Some e-poll books contain electronic data that was pre-loaded onto the device in static form and do not maintain an internet connection on election day, while others allow access to VRDs via a live internet connection.[16]

---

[12] Ibid.
[13] Ibid.
[14] http://uscode.house.gov/view.xhtml?req=(title:52%20section:21083%20edition:prelim)
[15] https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy
[16] Ibid.

Casting Votes

Direct recording electronic (DRE) voting machines. These devices are the voting machines themselves – where voters record their choices directly at a digital interface and a computer counts the (paper-free) vote. Voting machines with a mechanical lever are no longer in use.

Ballot-marking devices (BMDs). Some jurisdictions that do not use DREs use ballot-marking devices, where the voter selects candidates from an electronic interface and the electronic device physically marks a paper ballot accordingly. BMDs are one method of improving accessibility for blind and handicapped voters. These ballots are usually counted by optical scanners.

Optical scanners. In jurisdictions where voters hand-mark a paper ballot or use a BMD to cast their votes, ballots are usually fed into a scanning device to be "read" and counted. Scanning devices may be available on-site at each polling place, but some jurisdictions will bundle up their paper ballots and deliver them to a central location where they are scanned.

Counting, Reporting and Verifying the Vote

After the polls close, paper ballot votes may be counted manually; paper ballots may be scanned and counted digitally; and votes cast using electronic systems may be counted digitally.[17]

Voting tabulator machines. These devices are deployed at election precinct headquarters to aggregate the votes cast across the polling stations in a jurisdiction after the polls have closed. Administrators at a polling station will extract a removable media device (e.g., a flash drive) from their voting machines after polls have closed and physically deliver the device to the precinct headquarters so its data can be aggregated on the voting tabulator.

Election night reporting systems. The process by which election administrators transmit the county and state level totals to government websites. For example, in precincts using electronic DRE voting machines and centralized tabulators, administrators at a polling station will extract a removable media device (e.g., a flash drive) from their DREs after polls have closed and physically deliver the device to precinct headquarters so its data can be aggregated on the tabulator. The information from the tabulator is then exported to a reporting website.

Ballot reconciliation. Election officials use a variety of methods at the end of election day to ensure the various technology components of the election system see "agreement" as a check for system malfunctions or interference. For example, a polling station will compare the number of voters that signed in at the poll book with the number of votes cast as recorded by the tabulator.

Ongoing

Maintenance and programming activities. Private vendors of election technologies will use a variety of strategies to program the hardware and software before the point of sale and to maintain those systems with upgrades once they are in circulation. For example, vendors will

[17] https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

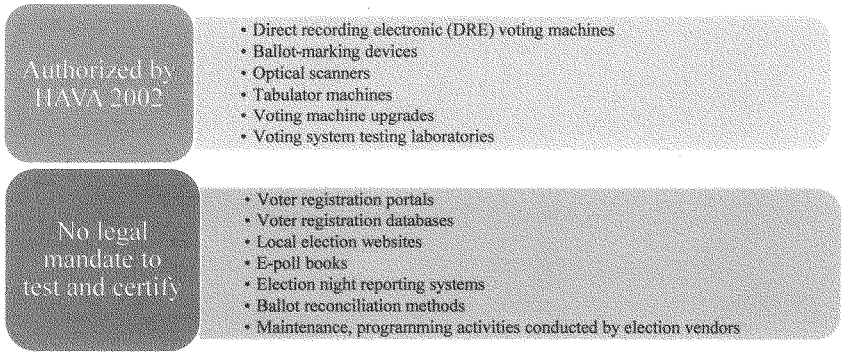
program an electronic DRE voting machine in advance of an election to display the candidates for that particular race.

What HAVA 2002 does not address

HAVA 2002 establishes federal responsibilities for testing, certification, training, technical assistance, grant-making and other activities related to voting systems. In turn, Section 301(b) of HAVA 2002[18] defines "voting system" as follows:

> (b) VOTING SYSTEM DEFINED.—In this section, the term "voting system" means—
> (1) the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used—
> (A) to define ballots;
> (B) to cast and count votes;
> (C) to report or display election results; and
> (D) to maintain and produce any audit trail information; and
> (2) the practices and associated documentation used—
> (A) to identify system components and versions of such components;
> (B) to test the system during its development and maintenance;
> (C) to maintain records of system errors and defects;
> (D) to determine specific system changes to be made to a system after the initial qualification of the system; and
> (E) to make available any materials to the voter (such as notices, instructions, forms, or paper ballots).

Under this definition, the legal mandate for NIST to assist in creating standards extends to only some of the election components described above.



[18] https://www.eac.gov/assets/1/6/HAVA41.PDF

Recent Incidents of Insecure Voting Infrastructure

In September 2017, the Department of Homeland Security contacted **21 states** to notify them that their election systems had been targeted by Russian hackers during the 2016 cycle.[19] A Senate Select Committee on Intelligence report that followed in May 2018 found that in at least six of the 21 states, "the Russian-affiliated cyber actors went beyond scanning and conducted malicious access attempts on voting-related websites."[20]

In May 2019, Special Counsel Robert Mueller released the *Report On The Investigation Into Russian Interference In The 2016 Presidential Election.*[21] The Mueller Report describes how Russian GRU officers "targeted individuals and entities involved in the administration of the elections. Victims included U.S. state and local entities, such as state boards of elections (SBOEs), secretaries of state, and county governments, as well as individuals who worked for those entities."[22] Russia also targeted "private technology firms responsible for manufacturing and administering election-related software and hardware, such as voter registration software and electronic polling stations." Special Counsel Mueller noted that this interference continued through the November 2016 elections.[23]

Special Counsel Mueller concluded his only public speech about the report by made emphasizing, "**there were multiple, systematic efforts to interfere in our election. That allegation deserves the attention of every American**.[24]"

Some of the incidents described below are presumably captured in the DHS count of 21 states.

- Two counties in **Florida** experienced breaches in their election networks during the 2016 election using spearfishing emails. Malware was also planted in systems at a manufacturer of election equipment, later identified as VR Systems.[25]

- In 2018 in **Johnson County, Indiana**, internet connections between e-poll books faltered, preventing e-poll books from tapping voter registration data and from communicating with one another. The lapse stopped voting entirely for four hours, with no extension of polling hours, and created an opportunity for a voter to vote twice in Johnson County.[26]

- In 2018, **Riverside County, California** saw unauthorized changes had been made to registered voters' party affiliations via internet access. Election officials were unable to identify the source of the changes as their systems did not track the IP addresses responsible.

---

[19] https://www.washingtonpost.com/world/national-security/dhs-tells-states-about-russian-hacking-during-2016-election/2017/09/22/fd263a2c-9fe2-11e7-8ea1-ed975285475e_story.html?utm_term=.31f42a3824a5
[20] https://www.intelligence.senate.gov/publications/russia-inquiry
[21] Full text of the Mueller Report: https://cdn.cnn.com/cnn/2019/images/04/18/mueller-report-searchable.pdf.
[22] Ibid page 50
[23] Ibid page 50
[24] https://www.justice.gov/opa/speech/special-counsel-robert-s-mueller-iii-makes-statement-investigation-russian-interference
[25] https://www.npr.org/2019/05/14/723215498/florida-governor-says-russian-hackers-breached-two-florida-counties-in-2016
[26] https://cha.house.gov/sites/democrats.cha.house.gov/files/documents/JLH%20CHA%20Election%20Security%20Testimony%20190508-FINAL%20%28002%29.pdf

- During the 2018 general election, **New York City** saw unprecedented lines to vote at numerous polling places as a result of jammed optical scanning equipment. It was later determined that high-humidity weather likely caused the machines to malfunction.[27]

- In June 2016, the **Illinois** Board of Elections network was hacked and intruders spent several weeks exploring the network, downloading the voter registration database and data about individual voters. The attackers then crashed a server, alerting officials of their presence.

- In 2016 the **Arizona** state elections website was breached by the same agent who attacked the Illinois Board of Elections. The intruders installed malware in the website.[28]

- During early voting for the 2018 general election in **Texas,** some electronic DRE voting machines deleted votes for Democratic candidates or switched them to Republican candidates. The machines in question were used in 78 of 254 Texas counties.[29]

- Early voters in **Georgia** in 2018 saw DRE machines deleting votes and switching them to other candidates. The machines where voters saw this occur were purchased in 2002.[30]

- In May 2018, the **Knox County, Tennessee** election website was hit with a distributed denial-of-service (DDoS) attack that crashed the website that displays election results.[31]

- In 2016, a vendor serving **Durham County, North Carolina** inadvertently created a pathway for attackers to breach the State Board of Elections' records by running an insecure remote-access software to service the county's voter registration database and e-poll books.[32]

- In September 2019, a researcher found an unlocked online repository containing what he said were "master passwords" for touchscreen voting machines in **North Carolina**. The repository also contained serial numbers for machines that had modems. State officials admitted the file should not have been publicly available online.[33]

- In late 2018, independent investigators found that the computer servers that provide the platform for **Wisconsin**'s reporting of elections results were running a service called FTP that enables access to sensitive information without a password.[34]

- The Wisconsin investigation also discovered that the servers powering **Kentucky**'s online voter registration were similarly exposed to tampering or exploitation via an FTP.[35]

---

[27] https://www.propublica.org/article/new-york-city-polling-places-midterms-2018-humidity
[28] Ibid..
[29] https://subscriber.politicopro.com/article/2018/11/voting-machine-errors-already-roil-texas-and-georgia-races-916984
[30] Ibid
[31] https://www.knoxnews.com/story/news/2018/05/02/knox-county-officials-investigating-election-night-cyberattack/572236002/
[32] https://www.politico.com/story/2019/06/05/vr-systems-russian-hackers-2016-1505582
[33] https://www.politico.com/newsletters/morning-cybersecurity/2019/06/10/cisa-budget-data-brokers-on-congressional-slate-this-week-648194
[34] https://www.propublica.org/article/file-sharing-software-on-state-election-servers-could-expose-them-to-intruders
[35] Ibid

Chairwoman SHERRILL. The hearing will come to order. Without objection, the Chair is authorized to declare recess at any time. Good afternoon, and welcome to a joint hearing of the Investigations and Oversight and Research and Technology Subcommittees. Ranking Member Norman and I had such a good experience working with Research and Tech last month during our transportation hearing that we thought we should do it again, so it's great to be here with Chairwoman Stevens and Ranking Member Baird, so thank you both, I appreciate it.

We are here today to talk about election security, and the various technologies and best practices that support it, and I want to start out by acknowledging something good. The experts tell us that the United States has, in fact, made enormous progress since 2016 toward protecting our election infrastructure. I applaud the Secretaries of State, the election officials, the poll workers, and the systems administrators across the Nation who have already been working to defy election interference. New Jersey, for example, is investing in a whole range of activities right now to prevent interference, including a pilot program for voter-verified paper trails.

But I remain worried about the enormous risks our election systems still face heading into 2020, and I have been really concerned about how attacks on our election system affect the American psyche. We have all seen anecdotes in the press about counties and States across the United States, where experts learn after the fact that an election system has been hacked. It is worth pointing out that we don't always see election systems actually being breached when they are targeted. Sometimes our systems work the way they're supposed to, and keep intruders from doing harm, and we should find comfort when we learn of a crisis averted, but for the most part we don't. These stories in the news allow us to see just how high the stakes are. They allow us to see how many ways there are to manipulate the system. These stories make the American people feel uncertain, and our peace of mind, our faith in the electoral process, is another casualty of interference.

There are few things more central to the American covenant than the safety and security of our elections, where citizens from all walks of life can cast their vote and know that it will be counted. Our foreign adversaries know this. The last two election cycles saw foreign interference in our election systems that tried to shake our faith in the U.S. election system, and in our fellow Americans. When I was in the Navy, I was a Russian policy officer, and I saw firsthand how the Russians worked to sow division here. We know the Russian intelligence service has already attacked our election infrastructure across a number of States, and we have every reason to believe these attacks will escalate during the 2020 cycle. The methods that foreign and domestic actors use to corrupt our elections are growing more sophisticated every day. When it comes to cybersecurity, the threat is constantly changing. It is our responsibility in Congress to help States arm themselves with advanced, adaptive strategies to prevent, detect, and recover from intrusions.

On a lighter note, I am delighted to welcome a special guest in the gallery today, Ms. Bianca Lewis. Bianca just finished the 7th grade in Phillipsburg, New Jersey. She is a coder and an inventor who runs her own blog dedicated to her adventures in STEAM.

That's science, technology, engineering, art, and mathematics. Bianca was also one of the young hackers featured at an exhibit that was hosted at last year's DEFCON technology conference in Las Vegas called Roots Asylum. At DEFCON, Bianca and other young people were able to exploit models of Secretary of State websites to delete content and change the voting results displayed. While the websites at DEFCON were models, and not part of any real life voting systems, they were designed with some of the known vulnerabilities that real life hackers have abused in recent years. I thank Bianca for being a leader for girls in tech and computer science, and for helping shine a light on cybersecurity and election infrastructure. It is so rewarding to see that the next generation is thinking big, and I'm glad that you and your family could be here today from New Jersey.

I'm also pleased to welcome the distinguished witnesses on our panel, three of whom contributed to the very important recent report from the National Academies on Securing the Vote. Thank you all for being here today.

[The prepared statement of Chairwoman Sherrill follows:]

Good afternoon, and welcome to a joint hearing of the Investigations and Oversight and Research & Technology Subcommittees. It's good to be here with Ranking Member Norman, Chairwoman Stevens and Ranking Member Baird once again.

We're here today to talk about election security and the various technologies and best practices that support it. And I want to start out by acknowledging something good:

The experts tell us that the United States has, in fact, made enormous progress since 2016 toward protecting our election infrastructure. I applaud the Secretaries of State, the election officials, the poll workers and the systems administrators across this nation who have already been working hard to defy election interference. New Jersey, for example, is investing in a whole range of activities right now to prevent interference, including a pilot program for voter verified paper trails.

But I remain worried about the enormous risks our election systems still face heading into 2020. And I have been really concerned about how attacks on our election system affect the American psyche. We have all seen anecdotes in the press about counties and states across the United States, where experts learn after the fact that an election system has been hacked. It is worth pointing out that we don't always see election systems actually being breached when they are targeted. Sometimes our systems work the way they are supposed to and keep intruders from doing harm.

And we should find comfort when we learn of a crisis averted. But for the most part, we don't. These stories in the news allow us to see just how high the stakes are. They allow us to see how many ways there are to manipulate the system. These stories make the American people feel uncertain. And our peace of mind, our faith in the electoral process, is another casualty of interference. There are few things more central to the American covenant than the safety and security of our elections, where citizens from all walks of life can cast their vote and know it will be counted.

Our foreign adversaries know this. The last two election cycles saw foreign interference in our election systems that tried to shake our faith in the U.S. election system - and in our fellow Americans. When I was in the Navy, I was a Russian policy officer and I saw firsthand how the Russians work to sow divisions. We know the Russian intelligence service has already attacked our election infrastructure across a number of states, and we have every reason to believe these attacks will escalate during the 2020 cycle. The methods that foreign and domestic actors use to corrupt our elections are growing more sophisticated every day. When it comes to cybersecurity, the threat is constantly changing. It is our responsibility in Congress to help states arm themselves with advanced, adaptive strategies to prevent, detect, and recover from intrusions.

On a lighter note - I am delighted to welcome a special guest to the gallery today, Ms. Bianca Lewis. Bianca just finished seventh grade in Phillipsburg, New Jersey. She is a coder and inventor who runs her own blog dedicated to her adventures in STEAM - that's science, technology, engineering, arts and mathematics. Bianca was also one of the young hackers featured at an exhibit that was hosted at last year's Def Con technology conference in Las Vegas called the R00tz Asylum. At Def Con,

Bianca and other young people were able to exploit models of Secretary of State websites to delete content and change voting results being displayed. While the websites at Def Con were models and not part of any real-life voting systems, they were designed with some of the known vulnerabilities that real-life hackers have abused in recent years.

I thank Bianca for being a leader for girls in tech and computer science - and for helping shine a light on cybersecurity in election infrastructure. It is so rewarding to see that the next generation is thinking big - about big challenges. I'm glad that you and your family could be here from New Jersey for today's hearing.

I am also pleased to welcome the distinguished witnesses on our panel, three of whom contributed to the very important recent report from the National Academies on Securing the Vote. Thank you all for being here.

Chairwoman SHERRILL. So the Chair now recognizes Mr. Norman for an opening statement.

Mr. NORMAN. Thank you, Chairwoman Sherrill, and Chairwoman Stevens, for convening this important hearing, and thank you for each of the witnesses for taking the time to give your testimony this morning. We're here today to review the security of the United States' election system technologies, and discuss research to ensure the security, the integrity, and the accessibility of America's election systems. Today's hearing provides an opportunity to learn how the Federal Government can support State and local governments as they work to secure elections through research, technology, standards, and voluntary guidance, without burdensome Federal mandates.

The 2000 Presidential election highlighted problems with punch card and lever voting systems, and brought to light new concerns about election integrity. To address these concerns, Congress enacted the *Help American Vote Act of 2002*, or better known as HAVA. HAVA provided money to the States to replace antiquated voting systems, established the United States Election Assistance Commission, or EAC, and required the National Institute of Standards and Technology (NIST) to provide technical support to the EAC to develop voluntary guidelines for voting systems.

My home State of South Carolina recently decided to upgrade voting systems, and serves as an example of how the process should work. South Carolina officials conducted a lengthy evaluation of several options, and ultimately determined that upgrading to a ballot marking device was the option that best met the needs of our State. And this is how it should be, State and local officials figuring out what is best for their community. As Federal policymakers, we must remember that administration of elections is inherently a function of State and local governments. We should listen to our local election officials, and provide the reasonable support necessary to bolster the security of election systems, and to efficiently and effectively administer elections throughout the United States. This requires a flexible and a dynamic approach to security that can be molded by jurisdictions across the country to fit their specific needs. A one-size-fits-all approach is simply impractical and unworkable.

I welcome the chance to hear from State and local election officials as we consider the issue of election system security, and look forward to their perspective on what role the Federal Government can play in ensuring that they have the information and support necessary to harden their election systems against present, and any future threats. We'll also hear today from representatives of

academia, the private sector, and the Federal Government, which provides us with the opportunity to learn more about technologies and innovations that will improve America's election systems today, as well as research underway that may bolster election system security in the future. It's hard to imagine an issue of greater importance to our democracy than the security of America's election system.

And while I appreciate that this Committee continues to approach critical issues of national importance in a bipartisan fashion, I would be remiss today if I didn't take the opportunity to highlight how partisan politics on the part of the House Democrat leadership has once again failed to proceed through regular order. Specifically, I'm disappointed but, you know, quite frankly I'm not surprised, as this is just another in a long list of political stunts by leadership's sudden decision to move H.R. 2722, the so-called *Securing America's Federal Elections Act*, to the floor this week without consideration by this very Science Committee, which rightfully received a referral on the bill. House Democratic leadership instead chose to rush this bill to the floor in order to satisfy far left progressives with yet another messaging bill that thankfully has absolutely no chance of being considered in the Senate. As today's hearings will demonstrate, the Science Committee has a crucial role to play in the consideration of any legislation that truly aims to improve the security of America's election systems. That being said, I look forward to a thoughtful and bipartisan discussion today of how we can improve the security of America's election systems now, and in the future.

I want to thank each of our witnesses for being here, and thank you, Madam Chair, for convening this all-important hearing. And I want to thank the Hyatts, who are here from my hometown, who have played a part in the elections in South Carolina, for being with us today. Madam Chair, I yield back the balance of my time.

[The prepared statement of Mr. Norman follows:]

Thank you, Chairwoman Sherrill and Chairwoman Stevens, for convening this important hearing, and thank you to the witnesses for your testimony this morning.

We are here today to review the security of U.S. election system technologies and discuss research to ensure the security, integrity, and accessibility of America's election systems.

Today's hearing provides an opportunity to learn how the Federal government can support state and local governments as they work to secure elections through research, technology, standards, and voluntary guidance, without burdensome Federal mandates.

The 2000 presidential election highlighted problems with punch card and lever voting systems and brought to light new concerns about election integrity. To address these concerns, Congress enacted the *Help America Vote Act of 2002* (or "HAVA").

HAVA provided money to the states to replace antiquated voting systems, established the U.S. Election Assistance Commission (or "EAC"), and required the National Institute of Standards and Technology to provide technical support to the EAC to develop voluntary guidelines for voting systems.

My home state of South Carolina recently decided to upgrade voting systems and serves as an example of how the process should work. South Carolina officials conducted a lengthy evaluation of several options and ultimately determined that upgrading to a ballot marking device was the option that best met the needs of the state.

And this is how it should be - state and local officials figuring out what is best for their community. As Federal policy makers, we must remember that administration of elections is inherently a function of state and local governments. We should listen to our local election officials and provide the reasonable support necessary to

bolster the security of election systems, and to efficiently and effectively administer elections throughout the United States.

This requires a flexible and dynamic approach to security that can be molded by jurisdictions across the country to fit their specific needs. A one-size-fits-all approach is simply impractical.

I welcome the chance to hear from state and local election officials as we consider the issue of election system security and look forward to their perspective on what role the Federal government can play in ensuring they have the information and support necessary to harden their election systems against present and future threats.

We will also hear today from representatives of academia, the private sector, and the Federal government, which provides us with the opportunity to learn more about technologies and innovations that will improve America's election systems today, as well as the research underway that may bolster election system security in the future.

It's hard to imagine an issue of greater importance to our democracy than the security of America's election systems. And while I appreciate that this Committee continues to approach critical issues of national importance in a bipartisan fashion, I would be remiss if I didn't take the opportunity to highlight how partisan politics on the part of the House's Democrat leadership has once again failed to proceed through regular order.

Specifically, I am disappointed-but quite frankly not surprised, as this is just another in a long line of political stunts-by leadership's sudden decision to move H.R. 2722, the so-called *Securing America's Federal Elections Act*, to the floor this week without consideration by the Science Committee, which rightly received a referral on the bill. House Democratic leadership instead chose to rush this bill to the floor in order to satisfy far-left progressives with yet another messaging bill that thankfully has no chance of being considered in the Senate.

As today's hearing will demonstrate, the Science Committee has a crucial role to play in the consideration of any legislation that truly aims to improve the security of America's election systems.

That being said, I look forward to a thoughtful and bipartisan discussion today of how we can improve the security of America's election systems, now and in the future.

Thank you again to our witnesses for being here today. And thank you madam chair for convening this important hearing.

I yield back the balance of my time.

Chairwoman SHERRILL. Thank you. The Chair now recognizes Chairwoman Stevens of the Subcommittee on Research and Technology for an opening statement.

Chairwoman STEVENS. Thank you, Chairwoman Sherrill. It's great to be here talking about election security and voting technology vulnerabilities, and we're certainly so grateful that we have the leadership in the House of Representatives willing to take on the severity of some of the election security breaches that we experienced in 2016, some of which have been long overdue, and the current Administration has failed to address. So, good afternoon, and welcome to this hearing.

Certainly the elections of 2016 showed us how vulnerable our election infrastructure can be to foreign adversaries who interfere in the very foundation of our democratic process, and this has begun a national conversation on the security and integrity of our U.S. elections. Most election authority rests with the States, but, as Mr. Norman recognized, Congress created a Federal role in election administration and security with the *Help America Vote Act of 2002*, known as HAVA. And, under HAVA, the National Institute of Standards and Technologies, NIST, which—the Subcommittee that I have the privilege of chairing on Research and Tech has oversight over—NIST was tasked with providing technical assistance and research to inform the development of voluntary voting systems—guidelines to be recommended to the Election Assistance

Commission, the EAC. HAVA provided hundreds of millions of dollars to States to buy new voting equipment, but some of those old machines are still in use today, and States, not having—being—or not being required to implement the voluntary voting system guidelines in the purchase of new voting machines, were left with a gap. Only 38 States and the District of Columbia use some of the parts of the Federal testing and certification program for purchasing new voting equipment.

With more than 10,000 election jurisdictions in the United States, there is certainly no one fit—no one-size-fits-all solution to election administration and security. In addition, most election administrators are well intentioned, but lack resources, awareness, and technical expertise. Cue the Federal Government. At the time of HAVA, voting technology was assumed to mean only the voting machine itself. Today, depending on the jurisdiction, a voter may be able to register online to vote, and have their name and address confirmed through an Internet connected electronic poll book, or e-poll book, at their polling site, in addition to casting their vote on an electronic machine. Unfortunately, many Americans still cast their vote on machines with no paper record.

I know we will hear from our experts today that all—with all the conveniences that the Internet and the 21st century technology provide, paper ballots are still the most secure. But even if we implement paper records everywhere, we are still left with the new security challenges posed with online registration and e-poll books. As a champion and a believer of 21st century technology, I am also still a champion for the analog skills that move us forward. In fact, every point of internet connectivity in the election system, including software development and updating, introduces a vulnerability. Security must be a priority at every step of our cherished democratic process. Free and fair elections are paramount.

Last year the National Academies issued a consensus study report titled "Securing the Vote: Protecting American Democracy". This report included several recommendations for improving election security, including the need for national standards for e-poll books, voter registration databases, ballot handling procedures, and audits. Finally, the report included a strong statement that the Federal Government has a responsibility to invest in research to protect the integrity of elections, which is part of what we are here today to discuss. I certainly could not agree more, and I am glad to know that, in addition to NIST, the National Science Foundation carries out computer science and social science research that could be applicable to election systems. There needs to be more coordination. We are fans of inter-agency work here on this Committee, and a more robust dedication of research dollars for this purpose. The 2020 elections are not far away. I look forward to our witnesses' insight on the Academies' report, and other important recommendations for this Committee to take up. Thank you, and I yield back.

[The prepared statement of Chairwoman Stevens follows:]

Good afternoon and welcome to this hearing to review U.S. election security and voting technology vulnerabilities. I look forward to hearing testimony from our distinguished panel of witnesses on this important topic.

The elections of 2016 showed us how vulnerable our election infrastructure can be to foreign adversaries who interfere in the very foundation of our democratic

process and began a national conversation on the security and integrity of elections. Most election authority rests with the states. However, Congress created a federal role in election administration and security with the *Help America Vote Act of 2002*, known as HAVA. Under HAVA, the National Institute of Standards and Technology, NIST, was tasked with providing technical assistance and research to inform the development of Voluntary Voting Systems Guidelines to be recommended to the Election Assistance Commission.

HAVA provided hundreds of millions of dollars to states to buy new voting equipment, and some of those old machines are still in use today. Further, states are not required to implement the Voluntary Voting System Guidelines in the purchase of new voting machines. Only 38 states and the District of Columbia use some part of the federal testing and certification program for purchasing new voting equipment.

With more than 10,000 election jurisdictions in the United States, there is no one size fits all solution to election administration and security, but these Guidelines are intended to have broad application. In addition, most election administrators are well intentioned but unfortunately lack the resources, awareness, and technical expertise to implement the vital security needs of today.

At the time of HAVA, voting technology was assumed to mean only the voting machine itself. Today, depending on the jurisdiction, a voter may be able to register online to vote and have their name and address confirmed through an internet-connected electronic poll book (or e-poll book) at their polling site, in addition to casting their vote on an electronic machine.

Unfortunately, many Americans still cast their vote on machines with no paper record. I know we will hear from our experts today that, with all of the conveniences that the internet and 21st century technology provide, paper ballots are still the most secure. But even if we implement paper records everywhere, we are still left with the new security challenges posed with online registration and e-poll books. In fact, every point of internet connectivity in the election system, including software development and updating, introduces a vulnerability. Security must be a priority at every step of our cherished democratic process.

Last year, the National Academies issued a consensus study report titled, ″Securing the Vote - Protecting American Democracy.″ This report included several recommendations for improving elections security, including the need for national standards for e-poll books, voter registration databases, ballot handling procedures, and audits. Finally, the report included a strong statement that the federal government has a responsibility to invest in research to protect the integrity of elections. I couldn't agree more, and am glad to know that in addition to NIST, the National Science Foundation carries out computer science and social science research that could be applicable to election systems. However, there needs to be more coordination and a more robust dedication of research dollars for this purpose.

The 2020 elections are not far away, I look forward to our witnesses' insight on the Academies' report and other important recommendations for actions this Committee can take to help.

Thank you and I yield back.

Chairwoman SHERRILL. Thank you, and the Chair now recognizes Dr. Baird of the Subcommittee on Research and Technology for an opening statement.

Mr. BAIRD. Thank you, Chairwoman Sherrill, and Chairwoman Stevens, for convening this day's hearing to review the security of U.S. election system technologies. Voting is a fundamental right of every American citizen, and ensuring the right to a safe and secure election is the responsibility of every Member of Congress. Without security, integrity, and accuracy in our electoral process, the foundation of our Nation, in fact, our democracy, is weakened. I look forward to hearing from our witnesses this afternoon about how the Federal Government can support State and local governments in ensuring safe and secure elections through research, technology testing, audits, and voluntary guidance.

As we all know, under our Constitution, the Federal system elects an Administration is, and should be, the responsibility of State and local governments. Our founders believed that government is more transparent, responsive, and accountable when it's

closest to the people, which is why the Constitution gave the responsibility of our elections to the States. To this end, Congress' role is to empower State officials to strengthen the security of their unique election systems, and effectively administer elections, not to try to dictate a one-size-fits-all. The *Help America Vote Act* established the Federal Election Assistance Commission, and requires the National Institute of Standards and Technology, NIST, to work with the Commission on technical, voluntary guidelines, and voting systems. These voluntary guidelines are an important tool for State and local elected officials to ensure the functionality and accuracy of the State's unique system. They allow the testing of voting systems to determine the basic functionality, accessibility, and security capabilities. They also offer flexibility, which is important, given the variation of election infrastructure from State to State.

I look forward to hearing from Dr. Romine about the most recent iteration of voluntary voting system guidelines, which is expected to be released soon. I believe it's also valuable that this Committee has the opportunity to hear what new and evolving challenges States are facing, and how States are using Federal resources to overcome unique challenges, including how and if these guidelines and protections are being effectively adopted. I expect Secretary Ziriax and Mr. Kelley will have particularly good insight into these challenges.

There's no doubt that there is a need for improved security of our elections. We know that at least 21 States have been targeted by foreign state actors prior to the 2016 U.S. election, and we know that Russian undertook disinformation campaigns on social media in that same election. This is troubling, but we must also acknowledge that no votes were changed in the 2016 election, and the 2018 midterm elections were secure, with a record number of voter participation. We must examine what we can learn from these past elections and improve upon them. We can make progress on this issue. I want to again thank Chairwoman Sherrill and Chairwoman Stevens for holding this hearing, and I hope that we will take a bipartisan look at the challenges of election security.

As my colleague, Ranking Member Norman, noted, this matter has not been addressed in a bipartisan manner thus far this Congress. But I hope this hearing will illustrate how progress can be made in keeping our Nation's elections secure, and free from interference. Thank you, and I yield back.

[The prepared statement of Mr. Baird follows:]

Thank you, Chairwoman Sherrill and Chairwoman Stevens, for convening today's hearing to review the security of U.S. election system technologies.

Voting is a fundamental right of every American citizen and ensuring the right to safe and secure elections is the responsibility of every Member of Congress.

Without security, integrity, and accuracy in our electoral process, the foundation of our nation - our democracy - is weakened.

I look forward to hearing from our witnesses this afternoon about how the federal government can support State and local governments in ensuring safe and secure elections through research, technology testing, audits and voluntary guidance.

As we all know, under our Constitution and federal system, election administration is and should be the responsibility of State and local governments.

Our Founders believed that government is more transparent, responsive, and accountable when it is closest to the people, which is why the Constitution gave the responsibility of our elections to the States.

To this end, Congress' role is to empower state officials to strengthen the security of their unique election systems and effectively administer elections, not to try to dictate a one-size-fits-all approach.

The *Help America Vote Act of 2002* (HAVA) established the federal Election Assistance Commission (EAC) and requires the National Institute of Standards and Technology (NIST) to work with the Commission on technical, voluntary guidelines for voting systems.

These voluntary guidelines are an important tool for state and local election officials to ensure the functionality and accuracy of that state's unique system.

They allow for the testing of voting systems to determine the basic functionality, accessibility, and security capabilities.

They also offer flexibility, which is important given the variation of election infrastructure from state to state.

I look forward to hearing from Dr. Romine about the most recent iteration of the Voluntary Voting System Guidelines, which is expected to be released soon.

I believe it is also valuable that this Committee has the opportunity to hear what new and evolving challenges states are facing and how states are using federal resource to overcome these unique challenges - including how and if these guidelines and protections are being effectively adopted.

I expect Secretary Ziriax and Mr. Kelley will have particularly good insight into these challenges.

There is no doubt that there is a need for improved security of our elections - we know that at least 21 states were targeted by foreign state actors prior to the 2016 U.S. election and we know that Russia undertook disinformation campaigns on social media in that same election.

This is troubling, but we must also acknowledge that no votes were changed in the 2016 election and the 2018 midterm elections were secure with a record number of voter participation.

We must examine what we can learn from these past elections and improve upon them. We can make progress on this issue.

I want to again thank Chairwoman Sherrill and Chairwoman Stevens for holding this hearing, and what I hope will be, a bipartisan look at the challenges of election security.

As my colleague, Ranking Member Norman noted, this matter has not been addressed in a bi-partisan manner thus far this Congress, but I hope this hearing will illustrate how progress can be made in keeping our nation's elections secure and free from interference.

Thank you and I yield back the balance of my time.

Chairwoman SHERRILL. Thank you, Dr. Baird. If there are Members who wish to submit additional opening statements, your statements will be added to the record at this point.

[The prepared statement of Chairwoman Johnson follows:]

Thank you Madam Chair, and I would like to join you in welcoming our witnesses this afternoon.

I'm glad we're holding this hearing today on such an important topic. The election system is decentralized and complicated. There are many different aspects of it that rely on technology in some form. As a result, there are numerous challenges and solutions to making sure our election system is secure, fair and accessible. Elections security, as we all know, is an active topic of conversation in Congress right now, as it should be. It is an urgent topic for our nation.

The Science Committee will do what it does best today - we will talk about the technology. My home state of Texas is a case study in how advanced technologies are both promising and perilous when it comes to the administration of elections. The 2018 election cycle saw a terrible episode in Texas in which malfunctioning electronic voting machines ended up changing some voters' selections from Democrat to Republican, and deleted some voters all together. This occurred across at least 78 counties. And the machines where this happened were paperless, which means it was impossible to go back and compare the voters' intent with what the device actually recorded. To underscore the gravity of what happened in 2018, the Texas Civil Rights Project issued a statement that this event "is threatening to call into question the entire election in Texas." To wit, in a court case that resulted from a similar episode in the state of Georgia, a judge ultimately decided that continued use of paperless systems can harm our constitutional rights to a free and fair election.

We were somewhat relieved to learn that cybersecurity experts believe that the voting machine anomalies in Texas can be attributed to old technology and not to

hackers. But it is easy to imagine how a bad actor might seek to take advantage of exactly this kind of vulnerability in Texas and across the country. On the other hand, Texas is looking at some exciting reforms. This year the Texas House is considering legislation that would implement automatic voter registration when eligible residents interface with the Department of Motor Vehicles. This proposal will not only make it more convenient for citizens to participate in the democratic process, it will also save money for state elections administrators and may help make the registration process more secure.

I hope that the experiences we have in Texas can be used as lessons learned for other states. In fact, I believe almost every state and jurisdiction is working hard to improve their systems and make them more secure and accessible. The Federal government has a role in shepherding the development of voluntary guidelines for secure elections and in providing technical and other assistance to state and local election administrators. We all need to learn from each other. Our very democracy is on the line.

I want to thank Chairwoman Sherrill, Ranking Member Norman, Chairwoman Stevens and Ranking Member Baird for holding this hearing, and I yield back the balance of my time.

[The prepared statement of Mr. Lucas follows:]

Thank you, Chairwoman Sherrill, Chairwoman Stevens, Ranking Member Norman, and Ranking Member Baird, for holding today's hearing.

The integrity and security of elections is fundamental to democracy in the United States. Americans must have confidence in the accuracy of election results, or we risk losing the public trust in government and our political system.

Although there is NO EVIDENCE to date that a single vote was changed in the 2016 or 2018 elections due to a cyberattack or foreign interference, we know that our adversaries are looking to erode public confidence in elections.

Prior to the 2016 federal election, a series of cyberattacks occurred on information systems of state and local election jurisdictions. The Federal Bureau of Investigation (FBI) announced that some state election jurisdictions had been the victims of cyberattacks aimed at exfiltrating data from information systems in those jurisdictions. The attacks appeared to be of Russian-government origin.

Although these attacks did not result in actual votes being changed, they served as a warning to Federal, State, and local officials that we must be vigilant about securing our elections.

The U.S. Constitution vests the responsibility of administering elections with State and local governments. However, the Federal government has an important role to play, in providing guidance and assistance to states on election systems. The Federal government can and should also work closely with State and local election officials to deal with foreign and domestic cyber threats.

Concerns with earlier versions of voting and election systems led to the passage of the *2002 Help America Vote Act* (HAVA). This Act requires the National Institute of Standards and Technology (NIST), over which our Committee has jurisdiction, to work with the Election Assistance Commission (EAC) on technical, voluntary guidelines for voting.

NIST plays an important role in conducting research on election systems and providing technical assistance and guidelines. NIST is a trusted partner by both industry and State governments. Because these guidelines are voluntary, States and private companies are more willing to share information with the agency, which results in better voluntary standards and guidelines. It is important that we support NIST in this work, and not erode their role in election security.

In Oklahoma, we have an election system that is secure, reliable, and provides timely results. I want to thank Mr. Paul Ziriax, Secretary of the Oklahoma State Election Board, for testifying today. Oklahomans can trust in the results of our State's elections, thanks to the thoughtful work of Paul and his staff. I look forward to hearing about how the Federal government can best support states like Oklahoma in their work, without creating mandates that are one-size-fits all.

What works for California might not work for Oklahoma, and I am glad we have two State and local election officials on the panel to hear what tools they need to administer secure elections in their jurisdictions.

The Science Committee has demonstrated over the last few months how Committees should work. Under the leadership of Chairwoman Eddie Bernice Johnson, we have been conducting hearings and moving legislation under regular order, and in a bipartisan and productive fashion, to make progress for the American people.

Unfortunately, the Democratic leadership of the House has chosen to ignore the Committee process, and rush two partisan bills to the floor in the name of ″election security,″ including H.R. 2722, a bill that will be considered on the House floor later

this week. That bill is partially in the Science Committee's jurisdiction, but leadership ignored regular order, and never gave our Committee members the opportunity to consider the legislation.

Unfortunately, that partisan bill goes far beyond securing elections - setting mandates on State and local governments for the administration of elections that have nothing to do with security or election integrity.

Republicans want to work with Democrats on election security. I hope this hearing demonstrates that commitment on both sides of the aisle and lays the groundwork for bipartisan legislation out of this Committee to update NIST"s election security activities.

Again, thank you to the chairs and ranking members for holding this hearing. I yield back.

Chairwoman SHERRILL. And, at this time, I would like to introduce our five witnesses.

First, we have Dr. Charles Romine is the Director of the Information Technology Laboratory at the National Institute of Standards and Technology, or NIST. And, Doctor, I'm not sure if I should offer you congratulations or condolences, I hear this is your 20th time testifying before us, so welcome again.

Mr. Neal Kelley is the Registrar of Voters for Orange County, California. Mr. Kelley is also a member of the National Academies of Science, Engineering, and Medicine, Committee on the Future of Voting. This committee contributed to the publication of the 2018 National Academies consensus study report titled, "Securing the Vote." Thank you for coming today.

Dr. Latanya Sweeney is a Professor of government and technology in the Department of Government at Harvard University's Institute for Quantitative Social Science. Thank you.

And then Dr. Benaloh is a Senior Cryptographer at Microsoft Research. Dr. Benaloh also contributed to the National Academies "Securing the Vote" report.

And, to introduce our final witness, I recognize Congresswoman Horn of Oklahoma's 5th Congressional District.

Ms. HORN. Thank you, Madam Chairwoman. I am honored today to be able to introduce not only our Election Secretary, but also one of my constituents from Oklahoma City, and I'm honored to be able to join you on this Subcommittee today on such an important issue.

Secretary Paul Ziriax has served as the Secretary of Oklahoma State Election Board since 2009, and as—in that capacity as our chief election official. He also serves as the Oklahoma—the Secretary of the Oklahoma Senate by way of a 1913 Oklahoma law that requires the Secretary of the Senate to also serve as the Secretary of the Education—or the Election Board.

Originally from Claremore, Ziriax has worked as a senior aide in the Oklahoma State Senate, Chief of Staff, and Press Secretary to a Member of Congress from Oklahoma, as a radio station music director and announcer. Ziriax is a member of the National Association of Election Directors, and the American Society of Legislative Clerks and Secretaries, and is a past appointee to the Oklahoma Capital Preservation Commission. He's an alumnus of Oklahoma State University in Stillwater, and finally, especially as related to this hearing today, I am proud of Oklahoma's election system because of our paper ballots, and a number of other security features that allow us to know the security and veracity of our elections, which is one of the things that we are talking about here today. So the work of Secretary Ziriax, and the staff of the Oklahoma

State Election Board, has been very important, and I'm glad that you could join us today, and look forward to your testimony.

Chairwoman SHERRILL. Well, thank you. Now I feel guilty I didn't give the rest of you the great intro. But, as our witnesses should know, you will each have 5 minutes for your spoken testimony. Your written testimony will be included in the record for the hearing. When you all have completed your spoken testimony, we will begin with questions. Each Member will have 5 minutes to question the panel. And let's start with you, Dr. Romine.

TESTIMONY OF DR. CHARLES H. ROMINE, DIRECTOR, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Dr. ROMINE. Chairwoman Sherrill, Ranking Member Norton, Chairwoman Stevens, Ranking Member Baird, and Members of the Subcommittees, I'm Charles Romine, the Director of the Information Technology Laboratory at the Department of Commerce's National Institute of Standards and Technology, or NIST. Thank you for the opportunity to appear before you today to discuss our role in what NIST is doing in election security.

For more than a decade, as directed by both the *Help America Vote Act of 2002*, or HAVA, and the *Military and Overseas Voter Empowerment Act*, NIST has partnered with the Election Assistance Commission, the EAC, to develop the science, tools, and standards necessary to improve the accuracy, reliability, usability, accessibility, and security of voting equipment used in Federal elections for both domestic and overseas voters. Under HAVA, NIST provides technical support to the Technical Guidelines Development Committee (TGDC), which is the Federal advisory committee to the EAC in areas such as the security of computers, computer networks, and computer data storage used in voting systems, methods to detect and prevent fraud, protection of voter privacy, the role of human factors in the design and application of voting systems, the remote access voting, including voting through the Internet.

This technical support includes intramural research and development in areas to support the development of a set of Voluntary Voting System Guidelines, referred to as the VVSG, or the Guidelines. The Guidelines are used by accredited testing laboratories as part of both State and national certification processes by State and local election officials who are evaluating voting systems for potential use in their jurisdictions, and by manufacturers who need to ensure that their products fulfill the requirements so they can be certified.

The Guidelines address many aspects of voting systems, including determining system readiness, ballot preparation and election definition, voting and ballet counting operations, safeguards against system failure, and protections against tampering, ensuring the integrity of voted balance, and protected data during transmission and auditing. Almost immediately following the adoption of Voluntary Voting System Guidelines 1.1, NIST established a set of public working groups to gather input from a wide variety of stakeholders on the development of the next iteration of the Guidelines, the VVSG 2.0. This approach pulled in subject-matter experts across the Nation, with 994 members across seven working groups.

Within the working groups, the cybersecurity working group has grown to 175 members, and it engages in discussions regarding the security of U.S. elections. Guidelines 2.0 addresses these evolving security concerns. It includes support for advanced auditing methods, as well as enhanced authentication requirements, and mandates two-factor authentication. The system integrity section in Guidelines 2.0 ensures that security protections developed by industry over the past decade are built into the voting system.

Other security issues to be resolved, beyond those mentioned in the Guidelines, include the need for regular and timely software updates and security patches. Networked communication is another important security issue currently under discussion. Many election jurisdictions rely on public telecommunication networks for certain election functions, such as reporting results to State agencies and media outlets on the night of the election. These connections, however brief, are a significant expansion of threat surface, and their security requires further study.

NIST participates in the DHS (Department of Homeland Security) Election Security Initiative federal partner roundtable, and kicked off the election profile of the cybersecurity framework effort in March 2019. NIST will hold workshops in July and in August to identify election processes and assets that need protection, threats from foreign control technology vendors, available safeguards, techniques that can detect incidents, and methods to respond and recover. The election profile will serve as a one-stop cybersecurity playbook that matches cybersecurity requirements with operational methodologies across all election processes, from voter registration through election reporting and auditing. The profile can be used by Secretaries of State, State and local election officials to identify and prioritize opportunities to improve their cybersecurity posture. NIST expects that an initial draft of the election profile of the cybersecurity framework will be available in the fall of 2019.

NIST is continuing to address election security by strengthening the VVSG for voting systems, such as vote capture and tabulation, and by working with our government partners, including the EAC, to provide guidance to State and local election officials on how to secure their election systems, including voter registration and election reporting systems.

Thank you for the opportunity to testify on NIST's work regarding election security, and I'll be pleased to answer any questions that you may have.

[The prepared statement of Dr. Romine follows:]

Testimony of

Charles H. Romine, Ph.D.

Director
Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

Before the
United States House of Representatives
Committee on Science, Space and Technology
Subcommittee on Investigations & Oversight and
Subcommittee on Research & Technology

Election Security: Voting Technology Vulnerabilities

June 25, 2019

Introduction

Chairwoman Sherrill, Ranking Member Norman, Chairwoman Stevens, Ranking Member Baird and members of the Subcommittees, I am Charles Romine, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss our role in what NIST is doing in election security.

NIST's Role in Cybersecurity

Home to five Nobel Prizes, with programs focused on national priorities such as advanced manufacturing, the digital economy, precision metrology, quantum science, and biosciences, NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In the area of cybersecurity, NIST has worked with federal agencies, industry, and academia since 1972, when it helped develop and published the data encryption standard, which enabled efficiencies like electronic banking that we all enjoy today. NIST's role, to research, develop, and deploy information security standards and technology to protect the federal government's information systems against threats to the confidentiality, integrity, and availability of information and services, was strengthened through the Computer Security Act of 1987 (Public Law 100-235), broadened through the Federal Information Security Management Act of 2002 (FISMA) (Public Law 107-347)1 and reaffirmed in the Federal Information Security Modernization Act of 2014 (FISMA 2014) (Public Law 113-283). In addition, the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

NIST develops guidelines in an open, transparent, and collaborative manner that enlists broad expertise from around the world. These resources are used by federal agencies and are frequently voluntarily used by other organizations, including businesses of all sizes, educational institutions, and state, local, and tribal governments, because NIST's standards and guidelines are effective, state-of-art and widely accepted. NIST disseminates its resources through a variety of means that encourage the broad sharing of tools, security reference data, information security standards, guidelines, and practices, along with outreach to stakeholders, participation in government and industry events, and online mechanisms.

The Role of NIST in Voting Systems

NIST's role in helping secure our Nation's voting systems draws on our expertise in providing measurements, working with standards development organizations, and the development of testing infrastructures necessary to support standards implementation.

Improving voting systems requires an interdisciplinary, collaborative approach. The systems must be accurate and reliable, yet cost-effective. They must be secure and usable. And, they

[1] FISMA was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347).

must be accessible to all voters, allowing them to vote independently and privately. Their design and the underlying standards must take into consideration the diversity of voting processes and ballots across the states. None of these can be considered in a vacuum. NIST expertise in testing, information security, trusted networks, software quality, and usability and accessibility provide the technical foundation for our voting systems work. Additionally, our experience working in multi-stakeholder processes is critical to success of NIST voting program.

For more than a decade, as directed by both the Help America Vote Act of 2002[2] (HAVA) and the Military and Overseas Voter Empowerment Act[3] (MOVE), the NIST Voting Program has partnered with the Election Assistance Commission (EAC) to develop the science, tools, and standards necessary to improve the accuracy, reliability, usability, accessibility, and security of voting equipment used in federal elections for both domestic and overseas voters.

Under HAVA, NIST is tasked with providing technical support to the Technical Guidelines Development Committee, Federal Advisory Committee to the EAC to which the Director of NIST serves as Chair, in areas such as the security of computers, computer networks, and computer data storage used in voting systems, methods to detect and prevent fraud, protection of voter privacy, the role of human factors in the design and application of voting systems, and remote access voting, including voting through the Internet. This technical support includes intramural research and development in areas to support the development of a set of Voluntary Voting System Guidelines (VVSG or Guidelines), which upon recommendation by the Technical Guidelines Development Committee are forwarded to the EAC for further consideration prior to adoption via a quorum of EAC Commissioners. The Guidelines are used by accredited testing laboratories as part of both state and national certification processes; by state and local election officials who are evaluating voting systems for potential use in their jurisdictions; and by manufacturers who need to ensure that their products fulfill the requirements, so they can be certified.

The Guidelines address many aspects of voting systems including determining system readiness, ballot preparation and election definition, voting and ballot counting operations, safeguards against system failure and protections against tampering, ensuring the integrity of voted ballots, protecting data during transmission, and auditing. Additionally, the Voluntary Voting System Guidelines tackles physical and systems-level security.

NIST Activities Related to Election Security

Voluntary Voting System Guidelines

The Guidelines is a set of specifications and requirements against which voting systems can be tested to determine if the systems meet required standards. On December 13, 2005, the EAC unanimously adopted the 2005 Guidelines, which significantly increased security requirements for voting systems and expanded access, including opportunities for individuals with disabilities to vote privately and independently. Version 1.1 of the Guidelines was unanimously approved by the Election Assistance Commissioners on March 31, 2015. Version 1.1 made the Guidelines

[2] Public Law 107-252, (Oct. 29, 2002), codified in relevant part at 52 U.S.C. 20901 *et seq.*

[3] Public Law 111-84, div. A, title V, (Oct. 28, 2009), codified in relevant part at 52 U.S.C. § 20311.

more testable and improved portions of the guidelines without requiring massive programmatic changes.

Almost immediately following the adoption of Voluntary Voting System Guidelines 1.1, NIST, in consultation with the EAC, established a set of a public working groups to gather input from a wide variety of stakeholders on the development of the next iteration of the Guidelines, entitled Voluntary Voting System Guidelines 2.0. This approach was consistent with NIST efforts in cloud and smart grid and served to address feedback from the Presidential Commission on Election Administration,[4] the EAC Standards Board, and the National Association of State Election Directors,[5] as well other subject matter experts across the Nation. There are currently 994 members across seven working groups, three of which are aimed at election process (pre-election, election and post-election), three groups focused on the technical underpinnings of the Guidelines (cybersecurity, usability and accessibility, and interoperability), and one that will address issues related to testing.

Election Security

The cybersecurity working group has grown to 175 members and engages in discussions regarding the security of U.S. elections. From the early 1900s, election administrators were primarily concerned with breaches of physical security, natural disasters, accidental errors, and events affecting public trust.

As U.S. election infrastructure has evolved, so have its security concerns, which today range from unauthorized attempts to access the voter registration systems of multiple states to errors or malicious software attacks. Guidelines 2.0 addresses these evolving concerns. It includes support for advanced auditing methods (such as risk-limiting audits) as well as enhanced authentication requirements. It mandates two-factor authentication for certain critical voting operations, including accessing administrative accounts, updating voting system software, performing aggregation of tabulation of ballots, enabling networking functions, and deleting or modifying the audit trail. Voting systems often use commercial off-the-shelf hardware and software. The system integrity section in Guidelines 2.0 ensures that security protections developed by industry over the past decade are built into the voting system.

Other security issues to be resolved, beyond those mentioned in the Guidelines, include the need for regular and timely software update and security patches. Networked communication is another important security issue currently under discussion. Many election jurisdictions rely on public telecommunications networks for certain election functions, such as reporting results to state agencies and media outlets the night of an election. These connections, however brief, are a significant expansion of threat surface and their security requires further study.

In January 2017, the Secretary of Homeland Security designated the Nation's election infrastructure as a critical infrastructure subsector of the Government Facilities Sector. Shortly thereafter, DHS established an Election Task Force to coordinate federal support to state and local governments regarding election security. NIST participates in the Election Task Force, recently recast as the Election Security Initiative Federal Partner Roundtable and is as an Ex

[4] https://www.supportthevoter.gov/

[5] https://www.nased.org/

Officio member of the Election Infrastructure Subsector (EIS) Government Coordinating Council, alongside our federal, state, and local partners. In support of these efforts, NIST is providing technical leadership in the creation of an Election Profile of the Cybersecurity Framework.

With our partners at DHS, NIST kicked off the Election Profile of the Cybersecurity Framework effort in March 2019 by establishing a joint subcommittee of the EIS Government Coordinating Council and the Sector Coordinating Committee (SCC). NIST co-leads this effort alongside DHS and the private sector chair of the Sector Coordinating Committee. To orient the efforts of the joint committee, NIST provided training on the NIST Cybersecurity Framework and profile development. In addition to the groundwork discussions occurring through bi-weekly meetings of the joint subcommittee, NIST will hold face-to-face workshops in July and August to identify election processes and assets that need protection; threats from foreign control of technology vendors; available safeguards; techniques that can detect incidents; and methods to respond and recover. The Election Profile will serve as a one-stop cybersecurity playbook that matches cybersecurity requirements with operational methodologies across all election processes, from voter registration through election reporting and auditing. The profile can be used by Secretaries of State, state and local election officials to identify and prioritize opportunities to improve their cybersecurity posture. NIST expects that an initial draft of the Election Profile of the Cybersecurity Framework will be available in the Fall of 2019.

Testing

NIST is responsible, under HAVA, for conducting evaluations of independent, non-federal laboratories and submitting to the EAC a list of the laboratories that NIST proposes to be accredited to carry out testing, certification, decertification, and recertification of voting systems.

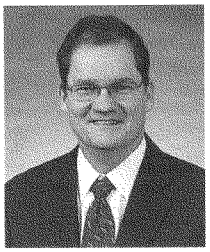
NIST developed "test assertions" for critical security, usability, accessibility and functional requirements under Voluntary Voting System Guidelines 1.0 and 1.1. It is anticipated that accredited voting systems laboratories will use these NIST-developed test assertions to achieve uniformity in testing among laboratories.

Conclusion

NIST is addressing election security by strengthening the Voluntary Voting System Guidelines for voting systems, such as vote capture and tabulation, and by working with our government partners, including the EAC, to provide guidance to state and local election officials on how to secure their election systems including voter registration and election reporting systems.

Thank you for the opportunity to testify on NIST's work regarding election security. I will be pleased to answer any questions you may have.

Charles H. Romine



Charles Romine is Director of the Information Technology Laboratory (ITL). ITL, one of six research Laboratories within the National Institute of Standards and Technology (NIST), has an annual budget of $150 million, nearly 400 employees, and approximately 300 guest researchers from industry, universities, and foreign laboratories.

Dr. Romine oversees a research program that cultivates trust in information technology and metrology by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for federal agencies and U.S. industry, supporting these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL supports NIST's mission, to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Within NIST's traditional role as the overseer of the National Measurement System, ITL is conducting research addressing measurement challenges in information technology as well as issues of information and software quality, integrity, and usability. ITL is also charged with leading the Nation in using existing and emerging IT to help meet national priorities, including developing cybersecurity standards, guidelines, and associated methods and techniques, cloud computing, electronic voting, smart grid, homeland security applications, and health information technology.

Education:
Ph.D. in Applied Mathematics from the University of Virginia.
B.A. in Mathematics from the University of Virginia.

Chairwoman SHERRILL. Well, thank you very much. And, Mr. Kelley?

TESTIMONY OF MR. NEAL KELLEY,
REGISTRAR OF VOTERS, ORANGE COUNTY, CALIFORNIA

Mr. KELLEY. Good afternoon, Chairwoman Sherrill, Chairwoman Stevens, Ranking Member Baird, Ranking Member Norman, and Members of the Subcommittee on Investigations and Oversight, and the Subcommittee on Research and Technology. My name is Neal Kelley. I'm the Chief Election Official, Registrar of Voters, for Orange County, California. Thank you for the invitation to speak today.

I'd like to address four specific things: The key findings of the National Academies of Sciences, Engineering, and Medicine's consensus study report; "Securing the Vote: Protecting American Democracy", the best practices used in Orange County, including the use of paper trails with voting machines, electronic poll books, and risk limiting audits; barriers States' and counties' encounter in the pursuit of enhancing election security; and how I believe Congress can further assist States and counties with securing election system technologies.

As a member of the National Academies' Committee on the Future of Voting, I have submitted the report highlights for Federal policymakers along with my testimony today. I would also like to share the insights I have gained as an election administrator. In the 2 decades following the 2000 Presidential election, numerous initiatives have been undertaken to improve our election systems. Although progress has been made, old and complex problems persist, and new problems emerge. Aging equipment, number one, the targeting of our election infrastructure by foreign actors, a lack of sustained funding dedicated to election security, inconsistency in the skills and capabilities of elections personnel, and growing expectations that voting should be more accessible and convenient, as well as secure, complicate the administration of elections in the United States.

Working together, NIST and the Election Assistance Commission have made numerous contributions to the improvement of electronic voting systems by providing critical technical expertise. The Voluntary Voting System Guidelines, otherwise known as VVSG, developed by the EAC in collaboration with NIST, are particularly important. Nevertheless, despite the critical roles that these agencies plays—play in strengthening election infrastructure, there is currently a very limited pool of ongoing financial support.

While one-time funding has been historically allocated, election cybersecurity is known to be an ongoing challenge that will require a constant effort to better understand threats and vulnerabilities. The National Academies' report recommends that the EAC and NIST, the architects, developers, and shepherds of the VVSG, continue the process of refining and improving the VVSG to reflect changes in how elections are administered; to respond to new challenges to election systems as they occur, such as the threat of cyber attacks; and to research how new digital technologies can be used by Federal, State, and local governments to secure elections. Our report further recommends that a detailed set of cybersecurity best

practices for State and local election officials be developed, maintained, and incorporated into election operations, and that the VVSG be periodically updated in response to new threats and challenges.

Electronic voting systems that do not produce a human-readable paper ballot of record are a particular concern, as the absence of a paper record raises security and vulnerability issues. Because of this, our report recommended that all elections should be conducted with human-readable paper ballots. We also recommend the use of risk limiting audits. An RLA is not considered to be performance audit, as it seeks to ensure accuracy that the reported outcome would be the same if all ballots were examined manually, and that any different outcome has a high likelihood of being detected and corrected. The National Academies' report also recommends that the use of the Internet, or any network connected to the Internet for a voter to cast a ballot, or the return of a marked ballot, should not be permitted.

There is no known technology that guarantees the secrecy, verifiability, and security of a marked ballot transmitted over the Internet. Voter registration databases are also vulnerable to cyberattacks, whether it is a standalone, or is connected to other applications. Presently, election administrators are not required to report any detected compromises or vulnerabilities in voter registration systems, and our report recommends that States make it mandatory for election administrators to report these instances when it occurs to the Department of Homeland Security, the EAC, and State officials.

As the fifth largest voting jurisdiction in the United States, Orange County, California is in the fortunate position of being able to allocate resources and staff to support pilot programs, and determine best practices for the use of paper audit trails, voting machines, and electronic poll books. On the matter of election security, in Orange County we remain closely connected to our local fusion center, and to information sharing and analysis centers. In addition, I routinely invite security experts to conduct audits and testing on our systems to identify vulnerabilities, and to propose solutions. Electronic poll books must meet high-level security requirements to be used in California, and my office has placed additional requirements on potential electronic poll book solutions. Data must be encrypted while in transmission, and while at rest. Nevertheless, not every election office has the resources that we have in Orange County. There are hundreds, if not thousands, of election offices where only a handful of dedicated staff are on hand to run their jurisdiction's elections. To share the knowledge and experience——

Chairwoman SHERRILL. Wrap it up quickly, please.

Mr. KELLEY. Going quickly. I released the 2018 Election Security Playbook for Orange County elections, and I have attached that to my written testimony.

Chairwoman SHERRILL. Thank you.

Mr. KELLEY. And thank you, and I look forward to your questions.

[The prepared statement of Mr. Kelley follows:]

ELECTION SECURITY: VOTING TECHNOLOGY VULNERABILITIES

Statement of

Neal Kelley

Registrar of Voters, Orange County, California

and

Past President, California Association of Clerks and Election Officials (CACEO);

Past President, National Association of Election Officials;

Past Chair, United States Election Assistance Commission (EAC) Board of Advisors;

Member, EAC Voting Systems Standards Board;

Member, Department of Homeland Security (DHS) Election Security Task Force (Government Coordinating Council);

Member, 2018 National Academy of Sciences, Engineering and Medicine's Committee on the Future of Voting: Accessible, Reliable, Verifiable Technology Committee

before the

The Subcommittee on Investigations & Oversight; and
The Subcommittee on Research & Technology

House Committee on Science, Space, and Technology

U.S. House of Representatives

June 25, 2019

Good afternoon, Chairwoman Sherrill, Chairwoman Stevens, Ranking Member Baird, Ranking Member Norman, and members of the Subcommittee on Investigations & Oversight and the Subcommittee on Research & Technology. My name is Neal Kelley and I am the Chief Election Official, Registrar of Voters for Orange County, California. Thank you for the invitation to speak at this joint hearing to address:

- The key findings of the National Academies of Sciences, Engineering, and Medicine Consensus Study Report, "*Securing the Vote, Protecting American Democracy*",[1] specifically as they pertain to the National Institute Standards of Technology (NIST).;
- The best practices used in Orange County, including the use of paper trails with voting machines, electronic pollbooks and risk-limiting audits;
- Barriers states and counties encounter in the pursuit of enhancing election security; and
- How Congress can further assist states and counties with securing election system technologies.

As a member of the National Academies of Sciences, Engineering, and Medicine's Committee on the Future of Voting, I would like to share the key findings of the committee's report, "*Securing the Vote, Protecting American Democracy*", as they relate to NIST. I have submitted the Report Highlights for Federal Policy Makers along with my testimony today. I would also like to share the insights I have gained as an election administrator.

[1] For the full report, please see https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy. This report was undertaken with grants to the National Academy of Sciences from the Carnegie Corporation of New York (#G-16-53637) and the William and Flora Hewlett Foundation (#G-2016-5031) and with funds from National Academy of Sciences' W. K. Kellogg Foundation Fund and the National Academies of Sciences, Engineering, and Medicine's Presidents' Circle Fund.

The National Academies' report begins with a discussion of the 2016 Presidential Election, which exposed new technical and operational challenges faced by state and local governments, the federal government, researchers, and the American public. Specifically, the 2016 elections showed that we must become more discerning consumers of information and become more proactive in our efforts to defend our election systems against bad actors who seek out opportunities to infiltrate and undermine the credibility of our election infrastructure. The 2016 Presidential Election made it clear that the federal, state, and local governments must work collaboratively to secure our election infrastructure and that we must discuss the threats to our elections candidly and apolitically.

In the two decades following the 2000 Presidential Election, numerous initiatives have been undertaken to improve our election systems. Although progress has been made, old and complex problems persist, and new problems emerge. Aging equipment, the targeting of our election infrastructure by foreign actors, a lack of sustained funding dedicated to election security, inconsistency in the skills and capabilities of elections personnel, and growing expectations that voting should be more accessible and convenient as well as secure complicate the administration of elections in the United States.

We must prevent efforts to corrupt our electoral process while continuing to administer elections for an electorate that is increasing in size and complexity. The threats and challenges will continue to grow, and the security of the American elections process will only be achieved through collaboration, cooperation, and the allocation of sufficient resources.

Working together, NIST and the Election Assistance Commission (EAC) have made numerous contributions to the improvement of electronic voting systems by providing critical technical expertise. The voluntary voting systems guidelines (VVSG), developed by the EAC in collaboration with NIST, are particularly important. Nevertheless, despite the critical roles that these agencies play in strengthening election infrastructure, the federal government currently provides limited ongoing financial support. While one-time funding has been historically allocated, election cybersecurity is known to be an ongoing challenge that will require ongoing efforts to better understand threats and vulnerabilities and develop strategies and solutions to defend and protect America's election systems.

As elections will likely involve the use of even more technology in the future, the committee's report called upon NIST to develop security standards and validation protocols for electronic pollbooks in addition to the standards and verification and validation protocols that the agency has developed for voting systems. The development of such standards is crucial, but limited funds and staff resources make it difficult for NIST to address these and other challenges involved in protecting our election infrastructure. If the challenges currently facing our election systems are ignored, we risk an erosion of confidence in our elections system and in the integrity of our election processes.

Our report recommends that the EAC and NIST — the architects, developers, and shepherds of the VVSG — continue the process of refining and improving the VVSG to reflect changes in how elections are administered, to respond to new challenges to election systems as they occur (i.e., cyberattacks), and to research how new digital technologies can be used by federal, state, and local governments to secure elections. Our report further recommends that a detailed set of cybersecurity best practices for state and local election officials be developed, maintained, and incorporated into election operations and that the VVSG be periodically updated in response to new threats and challenges.

VVSG was first adopted in 2005 to increase security requirements for voting systems and it augmented the 2002 Voting System Standards to address advancements in election practices and computer technologies. The next iteration occurred 10 years later in 2015 with the approval of VVSG 1.1, which enabled NIST to create test environments for the proposed changes. Almost immediately following the adoption of VVSG, it was clear that we cannot wait another 10 years for updated voting system guidelines and principles and the EAC and NIST began working on the next iteration, entitled VVSG 2.0. Rather than provide device-specific guidance as previous VVSG versions did, VVSG 2.0 has a new structure to provide high-level principles and guidelines on all functions that are incorporated into a device or devices that make up a voting system. In addition, VVSG 2.0 will include requirements to provide technical details necessary for manufacturers to design devices that meeting the established principles and guidelines and test assertions that allow laboratories to test a voting system against the prescribed requirements.

The draft guidelines also require software independence for all voting systems so as to allow for the determination of the correct outcome even if the software does not perform as intended. Our report echoed this principle, recommending that the computers and software used to prepare ballots should be separate from the computers and software used to count and tabulate ballots.

While many of the discussions related to elections revolve around cybersecurity, continued attention must be paid to modernizing our election systems. Our report recommends that NIST should establish Common Data Formats for auditing, voter registration, and other election systems. Through conformance with such standards, new election systems would be better protected against infiltration attempts.

Electronic voting systems that do not produce a human-readable paper ballot of record are of particular concern as the absence of a paper record raises security and verifiability issues. Because of this, our report recommended that all elections should be conducted with human-readable paper ballots. We further recommended that states mandate risk-limiting audits prior to the certification of election results. With current technology, this requires the use of paper ballots. Recounts and audits should be conducted by human inspection of the human-readable portion of the paper ballots. Voting machines that do not provide the capacity for independent auditing (e.g., machines that do not produce a voter-verifiable paper audit trail) should be removed from service as soon as possible.

Whether required by law or because local officials have independently adopted an audit requirement, most jurisdictions conduct audits after an election. Some audits focus on the processes followed by election officials, which are performance audits, but those do not check for the accuracy of election results. The report specifically recommends states mandate risk-limiting audits (RLA) prior to the certification of election results and all federal and state contests, and for local contests where feasible for that reason. An RLA is not considered to be a performance audit as it seeks to ensure accuracy that the reported outcome would be the same if all ballots were examined manually and that any different outcome has a high likelihood of being detected and corrected. Colorado was the first state in 2018 to conduct RLAs in a statewide election.

The report recommends that use of the Internet, or any network connected to the Internet, for a voter cast a ballot or the return or market ballots should not be permitted. There is no known technology that guarantees the secrecy, verifiability, and security of a marked ballot transmitted over the Internet. No matter how well constructed or prepared, it is impossible to anticipate and prevent all possible attacks through the Internet and we know that there are actors who look for vulnerabilities with the deliberate intention to compromise America's elections. Although cybersecurity is a never-ending challenge, best practices such as adopting state-of-the-art technologies and best practices more widely and developing new knowledge about cybersecurity will achieve stronger defenses against cyberattacks.

Voter registration databases are also vulnerable to cyberattacks, whether it is standalone or it is connected to other applications. Presently, election administrators are not required to report any detected compromises or vulnerabilities in voter registration systems. The report recommends that states make it mandatory for election administrators to report these instances when it occurs to the DHS, the EAC, and state officials. In Georgia, more than 6.5 million voter records and other privileged information were exposed due to a server error. The security vulnerability had not been addressed 6 months after it was first reported to authorities, even though it could have been used to manipulate the state's election system. This is exactly the kind of scenario that can be avoided if the proper agencies were notified and had an opportunity to act.

Since voter registration databases are increasingly being integrated with other databases, it is recommended that election administrators routinely evaluate the integrity of voter registration databases and the other databases they are connected to. In Illinois, Russian actors targeted and breached an online voter database in 2016 by exploiting a coding error. For three weeks, they maintained undetected access to the system. Ultimately, personal information was obtained on more than 90,000 voters. In California, hackers penetrated state registration databases and gained access to the personal information of a large number of voters and demanded ransom. Election infrastructure should not be at the mercy of hackers motivated by money or a desire to inflict chaos upon the American people. Strict standards and funding can be established to prevent the likelihood of similar instances in the future.

In addition to recommendations directed to the EAC and NIST, our report offers recommendations for the federal government, state governments, and election administrators and calls for research on voting that supports basic, applied, and translational research relevant to the administration, conduct, and performance of elections.

As the fifth largest voting jurisdiction of the nearly 9,000 voting jurisdictions in the United States, Orange County is in the fortunate position of being able to allocate resources and staff to support pilot programs and determine best practices for the use of paper audit trails (with voting machines and electronic pollbooks). I am pleased to share what my team and I have practiced and learned over the past 15 years as one of the leading election administration agencies in the country.

On the matter of election security, we remain closely connected to our local fusion center and to Information Sharing and Analysis Centers such as Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC). Information sharing in both directions is tremendously helpful for maintaining awareness of innovative digital tools and security threats or challenges. In addition, we invite security experts to conduct audits and testing on our systems to identify vulnerabilities and to propose solutions as necessary. To increase staff awareness of election security, staff participate in regular table top exercises with government and private partners. Staff are also required to take and pass an annual countywide cybersecurity training. When considering potential vendors for professional services, we maintain strict security requirements to ensure vendor integrity.

In addition, Orange County partnered with DHS on its "See Something, Say Something" campaign to encourage staff, volunteers, and voters to speak up when there is something suspicious. The DHS "See Something, Say Something" campaign logo was prominently displayed in poll worker training manuals, polling place set-up guides, and office materials and the campaign was discussed in in-person trainings that thousands of poll workers participated in.

Starting in 2006, California Elections Code section 19250 required the use of a Voter Verifiable Paper Audit Trail (VVPAT) for any electronic voting machine in California. Although Orange County is in the process of obtaining new voting equipment, we currently use a voting system (Hart InterCivic HVS 6.1) which contains a VVPAT printer, installed by my office, that has been certified for use in California. A VVPAT allows a voter to manually verify that the selections on the ballot reflect their intentions, regardless of whether the ballot is paper or electronic ballot. This is particularly helpful in a recount because the original paper record can be used to verify that the final tally is correct.

Electronic pollbooks must meet high level security requirements to be used in California, and Orange County has placed additional requirements on potential electronic pollbook solutions. Data must be encrypted while in transmission and while at rest. Mobile device management allows advanced remote management of pollbooks and includes the ability to remotely wipe all data from a pollbook if it were to be misplaced or stolen. Additionally, electronic pollbooks are never connected to voting systems. This "air gap" eliminates the capability of affecting voting machines via pollbooks.

In 2018 I chose to implement two risk-limiting audit (RLA) pilot programs in both the 2018 Primary and General Elections. These audits identified best practices and allowed us to share lessons learned with other county election officials and policymakers for consideration when developing post-election audit procedures and policies. While having a legacy voting system does not prohibit an elections agency from conducting a risk-limiting audit, I recommend that voting systems be updated in order to better support risk-limiting audits at a ballot comparison level. This added ability, included only in modern voting systems, allows jurisdictions to provide voters with increased confidence in election outcomes.

Orange County has a long history of supporting the movement toward risk-limiting audits:

- In 2007, Orange County participated in the California Secretary of State's Post-Election Audit Standards Working Group to evaluate the 1% manual tally and other post-election audit models.
- In 2010, Orange County conducted an RLA audit pilot and submitted findings to the EAC.

Orange County specifically conducted RLA pilots in 2018 in advance of being allowed to conduct RLAs in lieu of the currently mandated 1% manual tally starting with the March 2020 Primary Election. Additionally, we partner with academic institutions to review our methodology. We solicit feedback from institutions such as MIT, UC Berkeley, Princeton, and Caltech.

To share our experiences and best practices, I released the *2018 Risk-Limiting Audit Pilot Project Report* in April 2019. This report is available on our website. It includes a glossary of terms and basic outline of RLA procedures to help those new to the concept of an RLA to become familiar with it.

Having served as the Chief Elections Official in Orange County, California for the past 15 years, I have seen the election security landscape change dramatically. In the current landscape, the focus is on developing digital defense strategies against ongoing foreign state sponsored attacks that seek to undermine confidence in our democratic institutions. State and local election officials need broad support to protect America's election infrastructure. As the Academies' report states, "To fully address the challenges inherent in electronic election systems and to prevent foreign interference, federal, state, and local officials must adopt innovative measures to ensure that the results of elections reflect the will of the electorate." The failure to do so will result in unforeseeable and lasting damage to the American public's confidence in elections, which is the underpinning of the democracy we live in and pride ourselves in.

As you know, states and counties differ not only in geographic area and population size but also in terms of their access to resources, funding, and information. Yet, the election security challenges that local election officials face have no bearing on the size of their jurisdiction, access to funding and resources, and ability to mitigate or respond to such threats. My office is considered by many to be at the forefront of election innovation by virtue of its participation in working groups that communicate election security information, its participation in trainings, and its prioritization reviews of all processes and procedures so as to identify and resolve vulnerabilities and be resilient against on-going and expanding threats.

Nevertheless, not every election office has the resources that we have in Orange County. There are hundreds, if not thousands, of election offices where only a handful of dedicated staff are on hand to run their jurisdiction's elections fairly and securely. The lack of personnel in many of these small jurisdictions make it difficult to add additional responsibilities. Sending staff to trainings or bringing trainings to small or rural voting jurisdictions can be particularly challenging because it reduces the number of staff on hand at the elections office. The magnitude of what is involved in maintaining election security can be overwhelming to any individual seeking to expand their knowledge and remain abreast of the ever-changing field of election security. We must not lose sight of smaller jurisdictions that could benefit greatly from shared resources.

To share the knowledge and experience gained by being at the forefront of election cybersecurity, I released the *2018 Election Security Playbook: Orange County, CA Elections* to provide other local elections officials and the public with an opportunity to understand the role of election systems as critical infrastructure, to share core information security principles, and to identify critical threats and vulnerabilities. The *Playbook* is the only guide to be published from the perspective of a local election official. It provides scenarios and tips that are relatable to other local election officials seeking to build their election security knowledge and implement basic safeguards to protect election systems.

The *Playbook* was reviewed by the Department of Homeland Security, the Election Assistance Commission, and the Federal Bureau of Investigation and it is available to the public in the Orange County Registrar of Voters' website in our Election Library. The *Playbook* has been downloaded thousands of times and has been publicly shared by the Department of Homeland Security, the National Association of State Election Directors, and the Cybersecurity and Infrastructure Security Agency as a resource for election offices to use as a starting point in building their foundation in election security. I have included the *Playbook* as an appendix to my testimony.

Additionally, I am the Co-Chair of the Department of Homeland Security's Digital Networking Development Working Group. A newly formed working group, the Department of Homeland Security Digital Networking Development (DND) Working Group is a partnership between representatives from the government and private sectors tasked with reviewing and providing recommendations on the development and utilization of digital tools to both private and public members of the election infrastructure community. This working group seeks to evaluate digital tools intended to communicate critical information to help secure election infrastructure, share digital tools to partners in government and private sectors, and research innovative digital tools that support cybersecurity and protect election infrastructure.

The first of its kind, the working group seeks to serve as a clearinghouse for information on digital tools that support election security. Local election officials have found the numerous sources of election security information to be overwhelming. This makes it difficult to identify the most up-to-date and relevant information. This contributes to the challenge local election officials face in remaining current on the latest digital tools, threats, and challenges. I am grateful for our partnership with DHS in making this information available in a constructive way.

Congress has a unique ability to address issues affecting multiple states. It is incredibly challenging to coordinate resource and knowledge sharing amongst states and local jurisdictions. Congress can greatly assist states and counties with securing election system technologies by assisting in the standardization of information sharing and by providing funding for the digital tools, training, and staff resources necessary to secure our elections. States and local governments are ready to work with Congress to secure our elections, and agencies such as EAC and NIST, if given the opportunity, could build upon their research and standards to support the development of the digital tools necessary to provide election security.

Thank you and I look forward to your questions.

2018 ELECTION SECURITY PLAYBOOK

ORANGE COUNTY, CA ELECTIONS



Table of Contents

EXECUTIVE SUMMARY 4

INTRODUCTION 6

ELECTIONS AS CRITICAL INFRASTRUCTURE 7

CORE INFORMATION SECURITY PRINCIPLES 7

TOP THREATS AND VULNERABILITIES 8
- Threat of Foreign States 8
- Examples of Threats 9
- Potential Impacts to an Election 10

PREVENTATIVE MEASURES AND MITIGATIONS 10
- Security Mitigations and Controls 10
  - Categorizations of Security Controls 10
  - Examples of Specific Security Controls 11
- Voting System Security Controls 14
  - Information Integrity and Accuracy 15
  - Risk Limiting Audits 15
  - Voter List Maintenance 16
  - Early Voting Center Security 17
  - Electronic Poll Book Security 17
  - Chain of Custody Procedure 18
- Partnerships and Information Intelligence Sharing 19
  - Partnership with Orange County Agencies 19
  - Partner with Regional and Local Law Enforcement 19
  - Partnership with Federal Agencies 20

Collaborative Intrusion Detection and Prevention System 20
Partners of the OCROV Ring of Election Security 20

Cybersecurity Training & Awareness Program 21
Human Firewall 21

Application of the NIST Cybersecurity Framework 22
Identify 22
Protect 22
Detect 23
Respond 23
Recover 23
Defense in Depth 23

INCIDENT RESPONSE PLAN **24**
Threat Intelligence Services 25
Data Backup and Recovery 25
Rehearsing Responses to Incidents 26
Crew Resource Management 26

CURRENT AND FUTURE STATE **26**
Controls in Place 26
Plans for 2018 26
Future Plans 26

Executive Summary

A paradigm shift occurred in election security in 2016 when widely reported attempts were made to disrupt elections in the United States. In addition, there has been a great deal of attention on issues related to ballot integrity, voter registration systems, and ensuring the eligibility of voters.

As a result, Orange County has been aggressively pursuing security measures to protect the integrity of our elections. We believe a proactive "ring of security" is critical to safeguard the millions of ballots that are cast in Orange County during each election cycle.

The purpose of this physical and cybersecurity election playbook is to provide a guide to anticipate, mitigate and respond to physical and cybersecurity threats. As threats continue to increase and evolve, having a playbook is one of many pieces that will help to improve our security profile. Although threats are constantly changing, and incidents are unique, this playbook provides a guide and a set of best practices to be better prepared for threats and incidents. This playbook also provides a set of standards to reference as we continue to improve our current systems and implement new ones.

We have implemented physical and cybersecurity controls as outlined throughout this playbook, while incorporating extensive physical and cybersecurity training for our employees. There are also classified security measures in place to ensure that these mitigation efforts are not compromised.

Our office has already implemented many of the items addressed in this playbook, including the following:

- Physical security surveys were executed.
- Physical security improvements were put into action.
- Partnerships were established with federal agencies, local agencies, and information sharing centers.
- Administrative, technical and physical controls have been enhanced.
- An internal playbook and Incident Response Plan has been developed.

- Plans are in place to conduct risk limiting ballot-polling audits based on a random sample of ballots.
- Proactive list maintenance above and beyond statutory requirements continues.

Orange County will continue to focus our resources on the protection of our election systems, ballot integrity and overall election security. We remain diligent and proud of our involvement at the forefront of election security planning.



Neal Kelley
Registrar of Voters
Orange County, CA

Neal Kelley is an appointee of the U.S. Department of Homeland Security, Election Infrastructure, Government Coordinating Council (GCC) and serves as a member of the U.S. Election Assistance Commission (EAC) Board of Advisors and Voting Systems Standards Board and is a member of the National Academies of Sciences, Engineering, and Medicine's Committee on the Future of Voting.

Introduction

The Orange County Registrar of Voters (OCROV) is responsible for the management of elections for its over 1.5 million registered voters; in fact, there are more registered voters in Orange County than in 21 individual states. The OCROV security systems and controls are in place to enable secure, yet efficient execution of this mission. This public physical and cybersecurity plan was developed to ensure that the information provided by our systems and information remains confidential, available, and accurate. The OCROV is dedicated to protecting the integrity and authenticity of our data as well as the integrity of all votes cast.

The cybersecurity playbook provides clear, actionable tasks using tactical approaches to counter the growing number of cyber as well as physical threats. It is important that we take a strong, proactive approach to our security campaign efforts. This approach is a combination of strategies, best practices, along with cybersecurity policies and procedures to reduce our risks and to minimize and prevent threats.

The importance of a cybersecurity playbook is illustrated by the following quote from the Harvard Kennedy School:

> "The consequences of a cyber breach can be substantial and devastating. For the foreseeable future, cyber threats will remain a real part of our Election process. As democracy's front line, we must recognize the risk of an attack, develop a strategy to reduce that risk as much as possible, and implement response strategies for that moment when the worst happens. While no campaign can achieve perfect security, taking a few simple steps can make it much harder for malicious actors to do harm. Ironically, the most sophisticated state actors often choose the least sophisticated methods of attack, preying on people and organizations who neglect basic security protocols. That is our primary reason for creating this Cybersecurity Campaign Playbook.[1]"

1 Harvard Kennedy School (2017) Defending Digital Democracy / Version 1.3: Retrieved from https://www.belfercenter.org/sites/default/files/files/publication/Playbook%201.3.pdf

Elections as Critical Infrastructure

On January 6, 2017, the Secretary of the Department of Homeland Security (DHS), Jeh Johnson, designated the Election Infrastructure in the United States as a subsector of the existing Government Facilities Critical Infrastructure sector. This designation by DHS means that the Election Infrastructure has become a priority for cybersecurity assistance and protections that DHS provides to a range of private and public-sector entities. Election Infrastructure has been defined as storage facilities, polling places and centralized vote tabulation locations used to support the election process. It is also defined as information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and to report and display results on behalf of state and local governments. Critical Infrastructure is a major concern for cybersecurity threats and vulnerabilities.

Core Information Security Principles

The OCROV has adopted guiding principles that describe our security objectives, which we refer to as our core information security principles. The core information security principles are an integral part of our information security architecture. The principles are the basis for many of our efforts outlined throughout this document. Our office uses a principle referred to as CIA, which is defined as[2]:

> Confidentiality – Confidentiality refers to protecting sensitive information, such as Personally Identifiable Information (PII). Any two of the following data points together – a name with address, Social Security number, driver's license, etc. – are considered PII and must be protected as data assets. The principle of "least privilege" is the idea that only authorized individuals or systems should have access to information on a need-to-know basis. This principle is intended to prevent unauthorized disclosure of voter information, PII or other sensitive voter data.
>
> Integrity – Integrity refers to the prevention of unauthorized or improper modification of systems and information. Integrity includes the principle that information should be protected from intentional, unauthorized, or accidental changes. Controls are put in place to ensure that information is only modified

2 Tipton, Harold F. Official (ISC)2 guide to the CISSP CBK. Boca Raton, FL: CRC Press, 2010. Print.

through accepted practices. This is to ensure that data has not been altered.

Availability – Availability refers to the idea of minimizing downtime. We have controls in place to ensure that our data is highly available, redundant and replicated securely offsite. In case of a disaster, it is important to have plans in place to ensure business continuity while minimizing downtime and impact to voters, which is critical. Future planning will continue to include designing and building everything with redundancy in mind. In addition, disaster recovery policies are in place to overcome disasters such as power failures, fires, and other unplanned disasters. Secure back up of data is also important to make sure access to our data is not disrupted in the event of a disaster.

Top Threats and Vulnerabilities

In order to properly develop a security plan, the potential threats and exploits must first be identified. In the following section, we give examples of potentials and threats that we have identified.

The National Institute of Standards and Technology (NIST), in Special Publication SP 800-30 defines[3] threats as "the potential for a particular threat-source to successfully exercise a particular vulnerability."

NIST Special Publication 800-30 Rev. A defines vulnerability as "a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised accidentally, triggered or intentionally exploited and result in a security breach."

Threat of Foreign States

Foreign States are a significant threat because they have access to resources and technologies that make their cyberweapons more dangerous and difficult to defend against. A large amount of cyber threat intelligence data focuses on preventing a breach or a leak from happening; however, even with companies and governments spending more on network defense, breaches from Foreign States are still occurring. A proper defense strategy must be proactive and engaged. We need to combine technology and techniques to combat Foreign States that try to intervene in our elections and

3 NIST Special Publication 800-30 Revision 1 Retrieved from nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

disrupt our democracy. We must take strong actions to prevent interference including misinformation, phishing expeditions, and any other forms of meddling, mischief, and disruptions from Foreign States. Throughout this cybersecurity playbook, the threat from Foreign States is incorporated into the planning process.

Examples of Threats

We have identified examples of potential threats and exploits specific to elections, and later in this report, we will describe some mitigation strategies. Listed below are examples of identified threats:

- Computer virus
- Malware
- Breach of confidential information
- Denial of access
- Bomb threats and physical threats
- Phishing attack
- Hacking
- Social engineering
- Tampering of voting equipment
- Power outage
- Disgruntled poll worker or employee
- Fake information, including from social media
- Physical access to voting machines
- Lost access to voter database
- Voter registration tampering
- Vendor related threats

- Supply chain threats

Potential Impacts to an Election

The above threats must be addressed, because they can potentially impact an election by causing failures to meet election deadlines, causing failures to process results on-time, and causing overall failures of the voting system.

Preventative Measures and Mitigations

In order to address the threats and vulnerabilities listed above, our office implements preventative measures through security mitigations and controls.

Security Mitigations and Controls

Categorizations of Security Controls

Security requires a comprehensive strategy, consisting of multiple facets. Security mitigations can be classified by the types of controls necessary for a secure organization. The types of controls are[4]:

Administrative controls - Administrative controls are procedures implemented to define the roles, responsibilities, policies, and administrative functions needed to manage the environment. The employee hiring and separation procedures listed below are examples of the administrative controls we have in place.

Technical controls – Technical controls are electronic hardware and software solutions implemented to control access to information and information networks. The intrusion detection systems listed below are examples of the technical controls we have in place.

Physical controls - Physical controls protect the organization's people and physical environment, such as locks, fire management, gates and guards. The security cameras and badge access controls listed below are examples of the physical controls we have in place.

In our process of identifying preventative measures and mitigations for our systems, we

4 Tipton, Harold F. Official (ISC)2 guide to the CISSP CBK. Boca Raton, FL: CRC Press, 2010. Print.

attempt to address each of these categories of controls. This helps to ensure we are approaching physical and cybersecurity from a comprehensive perspective.

Examples of Specific Security Controls

Listed below are examples of specific security controls in place, which include examples of administrative, technical and physical controls.

Voting System

- "Air gap" mitigation – An "air gap" refers to the idea that the voting system is not connected to any other network at any other time, including local networks and the internet. Our office uses an "air gap" with our voting system, which is one of the most effective ways of mitigating security risks.
- Ballot creation security – The ballot creation team is located in a room with limited security access, multi-factor badge access, surveillance systems, and no network connections. The printed ballot contains a tint and watermark.
- Chain of custody – Strict chain of custody controls are in place for ballots and voting components.
- Ballot printing - Ballot printing is conducted in-house, mitigating the risk of relying on a vendor for ballot production.

Network Security

- Security Information and Event Management (SIEM) system – SIEM includes intrusion detection, vulnerability assessment, asset discovery and inventory, behavioral monitoring, and log management.
- Physical Security – Strict badge access control and alarm monitoring are important components of our physical security.
- Firewalls – Firewalls are used to protect our networks.
- Intrusion Detection/Prevention Systems – Intrusion detection and prevention systems help to detect attempts of unauthorized access.
- User login security controls – Requiring password complexity, and using least privileged access are important user security controls.

- Critical and security updates, and patch management – Applying security patches is a basic security measure.
- Legacy workstations – Minimizing the use of outdated Operating Systems and software, as well as replacing legacy systems.
- User account management – Immediately disabling unused accounts is a standard security practice.
- Center for Internet Security (CIS) benchmarks – We review their recommendations and utilize them when possible to harden our systems.
- Enforce strong passphrase policy – We enforce password complexity for user accounts.

Website Security

- Encrypted web communication – The website is viewed over a secure connection. Forms submitted by users are encrypted using SHA-xxx Cryptographic Hash Algorithm and utilizes SSL Web Security Certificates (Cryptographic Hash Management Latest Security Certificates).
- SQL injection – Web applications are periodically checked for SQL injection vulnerabilities.

Training and Personnel

- Employee hiring and separation procedures – Background checks are performed on new employees, and all are required to receive security training. Separated employees' accounts are promptly disabled, and badges are deactivated.
- Phishing campaign simulation – Phishing campaign with OCROV staff are periodically simulated in order to test the efficacy of our training.
- Cybersecurity training program – All employees must complete a professionally created cybersecurity training program. Supplemental training is also provided, and security updates are routinely given in staff meetings.
- Physical security accountability – Personnel are held accountable for enforcing physical security practices.

Administrative

- Business continuity plan – A business continuity plan is updated periodically.
- Policies and procedures – Policies and procedures are developed with cybersecurity in mind.
- Incident response plan – An incident response plan is developed in the event of a cybersecurity incident.
- RFP security review – When requesting bids or proposals from vendors, we are including strict security requirements from the vendors.

Physical

- Physical security improvements – Since 2016 (and through 2018) we have made numerous improvements as a result of recommendations from independent assessments.
- Enhanced physical security around election cycles – Security is provided by the Orange County Sheriff's Department on and around the election.
- Surveillance systems – Physical security is enforced with security cameras and other monitoring devices throughout our facilities.

Collaboration

- Collaboration at the federal level – We have developed a direct relationship with DHS, FBI, and the Election Assistance Commission (EAC).
- Collaboration at the local level – We have developed a relationship with our Orange County's Chief Information Security office, and the Orange County Intelligence Assessment Center (OCIAC).
- Increased collaboration around election cycles – Before and after the election, we enhance our security awareness and communication, including regular meetings with the County's security office, DHS, and the FBI.
- Cyber resilience self-assessment criteria report – We will be performing the cyber resilience self-assessment as provided by DHS.

User Level Security

- Improved malware detection - We are currently using endpoint protection that is pattern and behavior based.
- Email encryption - We currently have the ability to send encrypted emails when necessary.
- Email spam\virus filter - Systems are in place that prevent potentially malicious emails from being sent to the users.
- Email links - All links received by users in emails are checked for safety before a user can open the link.
- Data loss prevention - The County is in the process of enabling data loss prevention, which helps to prevent users from sending sensitive information that should not be sent.

Mobile

- Mobile encryption – Any mobile devices and laptops that contain sensitive data will be encrypted before deploying them outside the office.
- Mobile Device Management (MDM) – Mobile devices used, including electronic poll books, will have the ability to be managed remotely, including the ability to remotely wipe the data.

Public Information

- Comprehensive election information – We will continue to provide accurate information to voters through multiple channels, which can be used to counteract false information.

Overall Security

- Third party security audit – We are using a third party to conduct a cybersecurity audit, which can help to discover additional vulnerabilities.

Voting System Security Controls

The voting system currently used in Orange County is a Direct Record Electronic (DRE) voting system, with a Voter Verifiable Paper Audit Trail (VVPAT). In order for a voter to access a ballot at a polling place, a four-digit random access code is used for activation. The electronic voting booth and poll worker control system possess

only minimal functionality as compared to a fully operational personal computer, thus minimizing the risk of unauthorized system access and code modification. Furthermore, the voting system is a standalone system without connectivity to any external network or the internet, which makes unauthorized access from a network virtually impossible. Additional technical controls are in place and required in order for the voting system to be certified for use in the State of California.

Information Integrity and Accuracy

Important administrative controls are the extensive logic and accuracy audits that are conducted before the election to make sure the voting system is properly recording the cast vote records. After the election, random audits are performed manually to ensure the paper record matches the final tally. Paper audit trails allow us to compare totals and check the results against the votes verified by the voters.

Risk Limiting Audits

California does not currently require Risk Limiting Audits (RLA). However, as a component of our security plan for 2018, we will be conducting pilot RLAs to ensure that the integrity of the votes cast are true and correct. Computerized systems may produce incorrect results due to programming errors or deliberate subversion. Even hand counts may be erroneous. RLA audits systematically check the election outcomes reported by vote-counting systems.

Specifically, a risk limiting audit checks some voted ballots or voter-verifiable records in search of strong evidence that the reported election outcome was correct – if it was. Specifically, if the reported outcome (usually the set of winner(s)) is incorrect, then a risk-limiting audit has a large, pre-specified minimum chance of leading to a full hand count that reveals the correct outcome. A risk-limiting audit can stop as soon as it finds strong evidence that the reported outcome was correct. (Closer elections generally entail checking more ballots.)[5]

In addition to the required 1% manual tally (which is a hand-count of 1% of all ballots cast), in 2018 our office will be conducting RLAs in the form of ballot-polling audits based on a random sample of ballots. This will be reviewed by academics from Princeton University, Tufts University and the Massachusetts Institute of Technology (MIT).

5 California Risk Limiting Audits Working Group, Version 1.1, October 2012

Voter List Maintenance

Maintaining an accurate voter list is an important part of the cybersecurity playbook because it prevents widespread voter fraud, and ensures access for eligible Orange County voters. Our office has made a concerted effort in previous years to improve the accuracy of the voter database, but we also our continually looking for additional methods to improve our process of maintaining the voter list.

In 2018, we will be conducting the following list maintenance activities:

- Alternate Residency Confirmation – We send a postcard to all voters who have had no voting or registration activity for four years. If these voters do not respond, they remain in an inactive status, which means they do not receive any election materials in the mail.
- National Change of Address – We use change of address data provided by the Post Office (USPS) to update addresses of registered voters. This also helps us to identify and contact voters who may have moved out of Orange County, or the State.
- Third Party Data Provider – This is an activity that is not required by law, but we will conduct as an additional process to update our voter registration list. We utilize a credit reporting agency to find updated address information for voters who have not provided updated information through all other methods.
- DMV Address Change – We continually process change of address data provided by the Department of Motor Vehicles (DMV).
- National Deceased Voter Data – This is another activity that is not required by law, but we will conduct as an additional process to determine deceased voters. In addition to the deceased voter data provided by the State and the County, we use a service which matches voter information to national deceased records. This provides an additional step to locate voters who have deceased records throughout the entire country.
- First Time Federal Voters – Our office is updating its process to validate first time federal voters. This will improve efforts to ensure voters have provided proof of residence in Orange County.
- Statewide Voter Database – The Statewide Voter Database became the official

system of record for voter registrations in California in 2016. Orange County has taken a proactive role in utilizing this new system to improve the identification of voters that move within the State. As an example, we helped to implement a statewide policy that makes registration dates consistent, in an effort to better determine the most current registrations of the voters.

Early Voting Center Security

Securing access at remote early voting centers is critical. We ensure that Request for Proposals (RFPs) include stringent security requirements of the proposed system, as well as the vendor themselves. From a technical perspective, we include a multi-layered approach to ensure the data remains encrypted and secured at all times. We will be utilizing devices that have Federal Information Processing Standard (FIPS) certified components and data will remain encrypted from point-to-point at all times.

Physical security is also consideration when choosing a location to host early voting. Only facilities that provide adequate physical security are chosen to be early voting sites.

Electronic Poll Book Security

Electronic poll books used in early voting centers must have a high level of security applied. Listed below are examples of our security requirements for electronic poll books:

- Must be certified by the Secretary of State's office.
- Must have encrypted communication between all devices.
- Must use SSL encryption when appropriate.
- The database and other data must be encrypted at all times.
- Must be able to continue to operate in the event of loss of a connection.
- All devices must be shut down and physically secured when not in use.
- Devices will not store personal identifiable information.

Mobile Device Management

Mobile device management allows total control of securing and enforcing policies to tablets, smartphones, and other devices. Mobile device management allows us to

remotely wipe a device, use password enforcement, enable application whitelisting or blacklisting, use data encryption enforcement, control application distribution and software updates, and more.

Chain of Custody Procedure

Chain of custody procedures are used by the OCROV as an administrative control as part of its overall strategy to secure our voting system. The chain of custody procedures include the following:

- Voting booth controllers are secured within a locked caged area, under video surveillance until they are deployed for the election.
- A minimum of two people are present when the voting booth controllers are returned on Election Night.
- Chain of custody documents are used for an additional layer of auditing.
- Voting booth controllers are placed in a numerically sealed transportation box.
- Memory cards are numerically sealed in the voting booth controller.
- All voting equipment is tracked when deployed and returned to the OCROV.
- Election personnel sign chain of custody documents for voting equipment at distribution locations.
- Election personnel and polling place workers are required to check the security seals periodically and report any broken seals or suspicious activity to the OCROV.
- An OCROV driver is accompanied by a Deputy with the Orange County Sheriff's Department that returns voting booth controllers to the OCROV.
- An OCROV representative signs for equipment upon its return.
- Voting equipment is inventoried and placed in a secured, video monitored location.
- Voted memory cards are tallied in a room that allows for open observation.

Partnerships and Information Intelligence Sharing

Information sharing is critical in taking a proactive security approach and is an important part of our preventative measures and mitigations. Tactics, Techniques and Procedures (TTP) is an approach that is used within a cyber threat intelligence solution. TTPs can help with predictive or emergent risk, such as sharing of a zero-day exploit on the Dark Web. A zero-day attack is an attack vector that takes advantage of a security weakness before the vulnerability becomes generally known. There is no time or opportunity for detection because the attacker exploits the vulnerability before the threat is known. TTP is an effective method in helping to prevent zero-day attacks. The TTP method can help identify possible targets, provide threat analysis data, and help with mitigation process. This data or research is provided to us by multi-state sharing cybersecurity threat analysis partners. This section focuses on some of the ways our office employs the approach of intelligence sharing as one of the mitigation strategies of our security plan.

Partnership With Orange County Agencies

The OCROV has been proactive in communicating with the County security team, and they have expressed a commitment to assist the OCROV when needed.

Orange County's Chief Information Security Officer (CISO) and a cybersecurity joint task force meet monthly to review and discuss security topics that focus on information security countywide. We are working to update and refresh policies, standards, and guidelines, which are key components of an effective information security plan. To address the CIA principles of the technology, the County security team routinely conducts a series of assessments and penetration tests on County network infrastructure, systems, and data. The County security team has also expressed a commitment to establishing an in-depth defense methodology for its infrastructure, systems, and data.

Partner with Regional and Local Law Enforcement

We interface on a regular basis with regional (California Secretary of State, Criminal Investigations) and local (Orange County District Attorney's Office) law enforcement. We routinely, when appropriate, continue to refer cases to these agencies for investigations.

In addition to these resources, our office interfaces directly with OCIAC to obtain additional threat information, and to have OCIAC help recover from an incident, if necessary.

Partnership With Federal Agencies

At the Federal level, election systems are designated as critical infrastructure by the Department of Homeland Security (DHS). This designation ensures election systems receive top priority cybersecurity assistance from DHS. Additionally, our office is in direct communication with the FBI, DHS, and EAC. As an example, the Department of Homeland Security National Cybersecurity and Communications Integration Center provides OCROV weekly cyber hygiene assessment reports. This report is intended to provide our office information regarding our office's internet accessible networks and hosts. This report includes vulnerability scan results, new vulnerabilities detected and mitigated vulnerabilities on internet facing hosts. These federal partnerships also help with the defense of risks presented by Foreign States.

Collaborative Intrusion Detection and Prevention System

The Multi-State Information Sharing and Analysis Center (MS-ISAC) provides a security network monitoring service, which includes a near real-time automated system that identifies and alerts on traditional and advanced threats on a network, facilitating the rapid identification of threats and attacks.

Partners of the OCROV Ring of Election Security

MS-ISAC® Multi-State Information Sharing & Analysis Center®

NIST National Institute of Standards and Technology U.S. Department of Commerce

Homeland Security

Cybersecurity Training & Awareness Program

The OCROV has adopted the County policy of a mandated IT security and awareness training program, which is required to be completed by all employees on an annual basis. This provides employees with basic knowledge and tools that are instrumental in helping the County as a whole to combat cyber threats, including threats that have a social engineering component. The topics covered under the training program include:

- Ransomware
- Password Guidelines
- Safe Election Security and Protection Against Nation State Intrusions
- Social Engineering
- Phishing
- Physical Security
- Privacy
- Mobile Device Usage
- Malware
- Social media

Human Firewall

In any organization, cybersecurity is everyone's responsibility. Human error or targeted spear phishing has consistently been the root cause of publicized cyber attacks, and it is up to the OCROV leadership teams to weave security awareness into the culture of the organization. The term "Human Firewall" means employees, through education and cybersecurity training, are trained to detect, recognize, and report threats. The "Human Firewall" is the human shield of defense against possible social engineering attacks. Our approach is structured to change human behavior by thoroughly training our employees, including volunteer poll workers, to be cautious, and to be trained to recognize and report cybersecurity incidents. The decisions humans make are just as important as the software they use; therefore, the best approach consists of a clear employee cybersecurity program that includes awareness and focuses on continuous

training and education. Additionally, this cybersecurity training and awareness program needs to be more than just a routine requirement; instead, the concepts should be reinforced in order to change employee behavior. For example, email continues to be a significant vector of choice for malware; therefore, it is important that our employees are trained annually, in addition to being reminded in monthly meetings, to be mindful of the many forms of phishing attacks that come through professional and personal emails. Other aspects of the "Human Firewall" include background checks and setting standards for following good security protocols.

Security isn't just a technology issue; it's a personnel issue. Errant clicks, user error, and social engineering attacks such as phishing are some of the biggest threats. Educating and empowering our users to make safer choices is vital to creating a more sustainable and successful long-term defense.

Application of the NIST Cybersecurity Framework

The NIST Cybersecurity Framework is a widely adopted framework that provides an additional perspective to our approach to cybersecurity and was created by the public and private sectors working collaboratively. This framework is composed of the following five major functions:

1. IDENTIFY assets you need to protect.
2. PROTECT assets and limit the impact.
3. DETECT security problems.
4. RESPOND to an incident or be ready to respond with a plan.
5. RECOVER from an incident.

Identify

Our agency, with guidance from Orange County Information Technology (OCIT) enterprise security, has developed the skills to manage the cybersecurity risk to systems, assets, data, and capabilities. This covers areas such as risk assessment, asset management, and governance.

Protect

We have developed and implemented the appropriate safeguards to ensure delivery of services. These security mitigations and controls are outlined throughout this document.

Detect

We have implemented the appropriate systems to identify the occurrence of a cybersecurity event as soon as possible. The security mitigations and controls include items outlined in this document such as intrusion detection systems, and collaboration with other agencies are a part of this strategy.

Respond

OCROV, along with a cybersecurity joint task force, has developed a cybersecurity incident response plan. The plan addresses the appropriate actions in the event of a cybersecurity event. These actions include response planning, communications, analysis, mitigation, and future improvements learned from the incident. This plan is an internal secure document not designed for public distribution.

Recover

We have developed appropriate activities to restore any capabilities or services that are impaired due to a cybersecurity event or physical intrusion. A business continuity plan is also a component of this aspect of the framework. The focus is also to maintain resilience for the network and protect it from further attacks.

Defense in Depth

Defense in depth is an information assurance concept in which multiple layers of security controls or defenses are placed throughout network infrastructure to detect anomalies and unusual network traffic. Preparing for a breach is very important. Multiple layers of network security minimize gaps in protection. Examples of currently used protections at the OCROV are a robust firewall, intrusion prevention, and antivirus protection.

Countermeasures that are used to help defend the network are:

- Identify, minimize and secure all network connections.
- Harden systems by disabling unnecessary services, ports, and protocols.
- Enable available security features of systems used.
- Implement robust configuration management practices.
- Continually monitor and assess the security of the systems, networks, and interconnections.

- Building a "Human Firewall" by providing cybersecurity training, providing awareness and holding individuals accountable.
- Configure our firewall and other security settings to be more restrictive.

These countermeasures are items we will be continually reviewed in order to effectively protect systems and networks from cyber-based attacks. Although defense in depth measures do not (and cannot) protect all vulnerabilities and weaknesses in an environment, they are part of the larger, overall strategy.

Incident Response Plan

Cyber Incident Management in Orange County utilizes a lifecycle approach. The Cyber Incident Management Lifecycle is composed of serial phases: preparation, identification, containment, eradication, recovery, and follow-up. It is also composed of ongoing parallel activities: analysis, communication, and documentation. This lifecycle is derived from many standardized cyber incident response processes such as those published by NIST, as well as other authorities.

The following are descriptions of those actions that comprise OCROV's Cyber Incident Management Lifecycle:

- Preparation - Maintaining and improving cyber incident response capabilities.
- Identification - Confirming, categorizing, scoping, and prioritizing suspected cyber incidents.
- Containment - Minimizing loss, theft of information, or service disruption.
- Eradication - Eliminating the threat.
- Recovery - Restoring computing services quickly and securely.
- Follow-Up - Assessing response to better handle future incidents through utilization of reports, "lessons learned" and after-action activities, in addition to mitigation of exploited weaknesses to prevent similar incidents from occurring in the future.

The following are elements present throughout the Cyber Incident Management Lifecycle:

- Communication - Notifying appropriate internal and external parties and maintaining situational awareness.
- Analysis - Examining available data to support decision-making throughout the Cyber Incident Management Lifecycle.
- Documentation - Recording and time-stamping all evidence discovered, information, and actions taken from Identification through follow-up.

Direct contacts and methods of escalation are imperative to be defined as we prepare for any given election. In the event of an actual attack or incident, we ensure this information and the cybersecurity incident response plan are accessible. It is critical as we prepare and increase our cybersecurity presence, that all involved parties remain in frequent communication, coordination, and are well acquainted with our cybersecurity playbook plans.

Threat Intelligence Services

Threat Intelligence helps organizations understand the risks of the most common and severe external threats. Earlier in this report, we have described how we use partnerships and collaboration to help prevent and mitigate cybersecurity threats. We also utilize those partnerships to respond to incidents.

As an example, we have established a partnership with OCIAC. Not only do they help to identify threats before they occur, they also provide support to respond to an incident, and share the intelligence with other potentially affected entities.

Data Backup and Recovery

An important component of an incident response plan is to have a robust recovery plan, including the ability to restore and recover data after a major disaster. We monitor our backups closely, and we follow best practices in backing up and performing test restores of data. By simply following best practices, our backup and recovery strategy can be an effective defense against encryption and extortion attacks such as ransomware or other data loss.

Rehearsing Responses to Incidents

We will be periodically rehearing our responses to physical and cybersecurity incidents. This will help employees understand their responsibilities, as well as to refine the response plan based on findings from the rehearsals.

Crew Resource Management

Crew Resource Management (CRM) is a training program which encompasses a wide range of knowledge, skills, and attitudes including communications, situational awareness, problem-solving, decision making, and teamwork; together with each of the sub-disciplines that each of these areas entail. CRM training is conducted at the OCROV, and its concepts are reinforced by the Registrar of Voters. CRM empowers employees to respond, make decisions, and communicate effectively during an incident.

Current and Future State

Controls in Place

Our office has implemented physical and cybersecurity controls as outlined throughout this playbook. We have also established partnerships with federal and local agencies to assist with our efforts and to share information. We have incorporated extensive physical and cybersecurity training for our employees. We have also developed an incident response plan in order to be prepared to respond to an incident. There are additional security measures in place that are not shared with the public to ensure that these additional mitigation efforts are not compromised.

Plans for 2018

2018 is an election year, which means we will be required to execute on many of the planning efforts described in this playbook. Many of the controls that have been put in place will be acted upon as we approach the election. Additionally, we will utilize the partnerships we have established by increasing our frequency of communication and establishing checkpoints to evaluate our readiness before the elections.

Future Plans

Threats are constantly evolving, vulnerabilities are continually being discovered, and new systems are periodically implemented; therefore, the playbook must be used as a foundation and guide for the future. As we implement new systems and processes,

we must review this guide to ensure that we are continuing to adhere to our core information security principles, and applying security controls from all facets including technical, administrative and physical perspectives. As we will be updating our voting system in the near future, we will apply this playbook through the entire process beginning with procurement, continuing through implementation, and applying through future elections.



REGISTRAR OF VOTERS
1300 South Grand Avenure, Bldg. C
Santa Ana, CA 92705
714-567-7600
ocvote.com

REGISTRAR OF VOTERS
1300 South Grand Avenue, Bldg. C
Santa Ana, California 92705
(714) 567-7600
TDD (714) 567-7608
FAX (714) 567-7627
www.ocvote.com

OFFICE OF NEAL KELLEY
Registrar of Voters

Mailing Address:
P.O. Box 11298
Santa Ana, California 92711

Biography of Neal Kelley
Registrar of Voters

Neal Kelley is Registrar of Voters for Orange County, California, the fifth largest voting jurisdiction in the United States, serving more than 1.6 million registered voters. Kelley has served as the Chief Election Official since 2005 and has led the Registrar of Voters' office through the largest cycle of elections in the County's 130-year history. He has been the recipient of numerous state and national awards for election administration and is a past recipient of the the "Public Official of the Year" award by the National Association of County Recorders, Election Officials and Clerks.

Kelley is an appointee of the U.S. Department of Homeland Security Election Security Task Force (Government Coordinating Council (GCC), which helps to oversee the protection of the nation's election infrastructure. He also serves as a member and past chair of the U.S. Election Assistance Commission (EAC) Board of Advisors and is a member of the EAC Voting Systems Standards Board as well as the Technical Guidelines Development Committee (TGDC). In addition, he served as a member of the 2018 National Academies of Sciences, Engineering, and Medicine's Committee on the Future of Voting.

Kelley is the past president of the California Association of Clerks and Election Officials (CACEO), and is the past president for the National Association of County Recorders, Election Officials and Clerks (NACRC).

Kelley earned a Bachelor of Science degree in business and management from the University of Redlands and an M.B.A. from the University of Southern California.

Chairwoman SHERRILL. Thank you. I appreciate it. Dr. Sweeney?

TESTIMONY OF DR. LATANYA SWEENEY,
PROFESSOR OF GOVERNMENT
AND TECHNOLOGY IN RESIDENCE,
DEPARTMENT OF GOVERNMENT, HARVARD UNIVERSITY,
INSTITUTE OF QUANTITATIVE SOCIAL SCIENCE

Dr. SWEENEY. Thank you, Chairwoman Sherrill, Ranking Member Norman, Chairwoman Stevens, Ranking Member Baird, and Members of the Committee. I'm not going to—I presented a written testimony I'm not going to read from, and instead like to give you just some highlights. Let me first tell you a little bit about myself. I have a Ph.D. in Computer Science from MIT. I'm a Professor of government at Harvard University, and I was the former Chief Technology Officer of the Federal Trade Commission. For the last 20 years, my research mission has been to scientifically investigate and reveal unforeseen consequences of technology and its impact on society. I put names to health data that was supposed to be anonymous at—and that's cited in the preamble of HIPAA (*Health Insurance Portability and Accountability Act*), and it led to a new field of study called data privacy. I documented adverse racial discrimination in online ad delivery that's led to a new area of computer science study called algorithmic fairness. I trained students to be these same type of technologists to work in the public interest, and my students have improved practices at CMS (Centers for Medicare and Medicaid Services), Facebook, Airbnb, just to name a few.

In 2016, we gathered together 50 computer scientists, and social scientists, and civil society organizations, and said, what are the most pressing problems? They made a list of 75. We then asked them to tell us which problem did they think was the most important for us to investigate for the year? They said elections. It was January 2016, and we began doing just that. We found different kinds of problems around misinformation campaigns, and things like that on the Internet they got—that were brought to our attention.

Eventually, though, we began realizing how broad the election system is. The surface area of it is huge. Every one of those boxes has its own nature of a vulnerability. And we are only—and the rest of my talk is only going to talk about what's in that upper left corner. It was motivated by what happened in Riverside County during the primaries in 2016, in which Republican—it was a close primary. Republicans showed up, and instead of getting a Republican ballot, they got everything but—many—hundreds of them got everything but a Republican ballot. There was no break-in, there was no database breach, it just seemed like somebody changed all these records through the online system.

And so this idea that you could just change a voter's address, which changes their polling place, which could disenfranchise voters, not—in a primary, but just in the general election, and there are other ways too, that if you impersonate a voter, and you could go online, you could make a big difference, whether you wanted to make a local impact on a local election, whether you wanted to shave points off of an election, or whether you wanted to disrupt the election altogether. So that gave us a set of research questions,

and we dug in. We found 35 States, and the District of Columbia, had a website in which a person could change their voter registration online. These were not always voter registration websites. Many of them were also from the Motor Vehicle Division as well.

As you can see, the big problem here is, how does the State know who you are? In the case of Delaware, it—using this system, it was the first name, last name, date of birth, and zip code. But there are many places where I could find the name, date of birth, and zip code of people who live in Delaware. That—an alternative that used the driver's license and date of birth is another example from Alabama. This is the summary for all of the websites that we found, and the information that they require. Most of them require some combination of demographics, like name, or date of birth, or maybe address. Some of them require some government-issued number, like a Social Security Number (SSN), or a part of it, or a driver's license number. None of them necessarily require all of them, or they were the same.

Second question, though, is where would you get this data? And we found no shortage of the availability of the data. You could buy voter lists directly, you could buy voter lists from brokers that had a lot of the information. Some voter lists were just posted freely online. We surveyed about 500 popular data brokers to get SSNs and other kind of information, and we went on the dark web and found that you could find a disturbing amount of information also, including all of the Social Security Numbers of Americans.

At the time, 11 of those websites had captchas, these ways to try to figure out who you were, but in 2016 every captcha, including the Google captcha you see at the bottom, could be automated to be defeated. So with people who had virtually no experience, with about one page of Python code, you could automate an attack, and the cost of doing that, including the virtual machines to do it, and to weight its time, turned—if I wanted to shave 1 percent of the voter information off of the voters from that—from those locations, it would be $24,000 across all of them. If I use name sources. It drops to 10,000 if I was willing to also use dark net information as well. We're not saying that it did happen. We're just saying that this is—it's possible to happen, and it's a real vulnerability. Homeland Security had recommended this kind of vulnerability assessment. We're happy that we were able to participate, and we are updating now as to what has been the response.

I'd better stop there. Thank you.

[The prepared statement of Dr. Sweeney follows:]





Harvard University | Data Privacy Lab

Latanya Sweeney, PhD
Professor of Government and Technology in Residence
Director, Data Privacy Lab
Institute for Quantitative Social Science

1737 Cambridge Street, K310
Cambridge, MA 02138
(617) 496-3629 latanya@fas.harvard.edu
latanyasweeney.org | dataprivacylab.org

June 24, 2019

The Honorable Mikie Sherrill, Chairwoman
The Honorable Haley M. Stevens, Chairwoman
U.S. House Subcommittee on Investigations & Oversight
U.S. House Subcommittee on Research & Technology
2318 Rayburn House Office Building
Washington, DC 20515

Re: Hearing on Election Security: Voting Technology Vulnerabilities

Dear Chairwoman Sherrill and Chairwoman Stevens:

I write to you in advance of the hearing on "Election Security: Voting Technology Vulnerabilities." I appreciate your interest in securing websites that maintain voter information. I was the lead author on a scientific paper that surveyed vulnerabilities in voter information websites in 2016[1]. My co-authors, Ji Su Yoo and Jinyan Zang, work with me on the Technology Science Initiative, in the Institute for Quantitative Social Science at Harvard University. We welcome your leadership on this critical issue and look forward to working with you and your staff.

In 2016, we conducted a series of scientific investigations into ways an attacker could use technology in an attempt to adversely impact elections. We found misinformation about polling place locations, which by November were corrected.

We also found websites for 35 states and DC in 2016 that were vulnerable to voter identity theft attacks: an imposter could submit changes to voter registration information. An imposter needed a combination of voter's name, date of birth, gender, address, Social Security Number, or Driver's License Number.

Relevant data could be acquired from government, data brokers, or darknet markets. Total cost of an automated attack against 1percent of all vulnerable voter registrations nationwide ranged from $10,081 to $24,926 depending on the data source used. States cost less, e.g., $1 for Alaska and $1,020 for Illinois.

A voter identity theft attack could disrupt an election by imposters submitting address changes, deleting voter registrations, or requesting absentee ballots.

[1] Sweeney L, Yoo J, Zang J. Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections. *Technology Science*. 2017090601. September 06, 2017. Version 2. https://techscience.org/a/2017090601

Voter Identity Theft

Could an attacker impact U.S. elections by merely changing voter registrations online? This reportedly happened during the 2016 Republican primary election in Riverside County, California. What about elsewhere? We surveyed official voter record websites for the 50 states and the District of Columbia and assessed the means and costs for an attacker to change voter addresses. Relatedly, an attacker could also change party affiliations, delete voter registrations, or request absentee ballots online. A voter whose address was changed without her knowledge, for example, in most states would have a polling place different than expected. On Election Day, when she appeared at her presumed polling place, she would have been unable to cast a regular vote because her name was not on the precinct's register. She may have been turned away or given a provisional ballot, and in many cases, a provisional ballot would not count. Perpetrated at scale, changing voter addresses, deleting voter registrations, or requesting absentee ballots could disenfranchise a significant percentage of voters, and if carefully distributed, such an attack might go unnoticed even if the impact was significant. So, how practical is it to submit false changes to voter registrations online?

In summary, we found that in 2016, the District of Columbia and 35 of the 50 states had websites that allowed voters to submit registration changes. These websites determined whether a visitor was an actual voter by requesting commonly available personal information. Some websites gave multiple ways for a voter to self-identify. Of these, {name, date of birth, address} was required in 15, {name, date of birth, driver's license number} was required in 27, and {name, date of birth, last 4 SSN} was required in 3. We found that an attacker could acquire the voter names, demographic information and government-issued numbers needed to impersonate voters on all 36 websites from government offices, data brokers, the deep web, or darknet markets.

Overall, the total cost of an attack in 2016 varied based on the number of voters to impersonate, data sources used, whether the websites had CAPTCHAs, and specific states of interest. We found that the practical costs of changing 1 percent of the voters on all 36 websites could range from $10,081 to $24,926 depending on whether the attacker used data from government, data broker, darknet or other sources. Costs for an attack on a specific geographical area or state were much less, such as $1 for Alaska or $1,020 for Illinois. Back office processes and election practices, which varied among states, could have possibly limited attack success rates.

Fundamental Cybersecurity Vulnerabilities

Usually "cybersecurity" focuses on ways an attacker can break into a system or steal the credentials of those administrators and officials who use the internals of the system. Once inside, the attacker has open access to the files and systems. For this reason, perimeter security that surrounds the stored information is critical. These can be addressed through traditional computer security best practices, including but not limited to those proposed by the Help America Vote Act (HAVA), the Voluntary Voting Systems Guidelines (VVSG) by the National Institute of Standards and Technology (NIST) and the Election Assistance Commission (EAC).

However, I want to point out that many government websites have unique security concerns that go beyond the ability to secure the perimeter. Additional vulnerabilities exist because the intended users of many government systems are members of the public who identify themselves to the systems using personal information that is also widely available. For example, the State of Delaware had a website for voter's to change their voter registration information online. A voter identifies himself to the system using {name, date of birth, 5-digit ZIP code}. The voter knows this information, but unfortunately, we showed that this same information was readily available from voter lists, data brokers and on the dark web. An attacker could impersonate a voter at scale on these websites to impact elections. Different state websites used different combinations of personal demographics and government issued identifiers, including Social Security numbers and driver's licenses. But all the combinations of information requested were available to an attacker. Even with perfect perimeter security afforded by traditional cybersecurity, an attacker could still commit "voter identity theft" and change voter records at scale through automated means inexpensively.

Assistance Congress Could Provide to Assist States and Counties in Securing Websites

Our findings identify the nature of the problem, but they also suggest best practices to limit or thwart voter identity theft.

In our paper, we computed the costs of changing one percent of the voter records at each website. Costs included the acquisition of the specific pieces of information needed to impersonate voters at the state website and the costs of using virtual machines to automatically change different records slowly over time to avoid human detection. The costs varied significantly among the states: Alaska was $1, Delaware was $7, and Ohio $330, as examples. The most expensive state was Texas at $3,059. The key characteristic that the Texas website had that made it more difficult to impersonate its voters was a serial code that appeared on the face of a driver's license that could not be computed from the demographics itself. Texas voters had to enter this code, but this code was not available from data brokers who provided driver license numbers. Impersonating Texas voters online required images of actual Texas driver's licenses, which we did find on the darknet. Clearly, using this number helps thwart identity theft.

One of the reasons automated attacks were inexpensive was because few websites had those annoying pop-up boxes that attempt to stop automation. CAPTCHAs as they are termed, request selecting a subset of images, entering text from an image, or performing some other task that should be easy for a real human to perform but difficult for an automated script to achieve. CAPTCHAs help defeat voter identity theft by limiting the speed of how many voters could be impersonated in a time period.

Eleven (31 percent) of the 36 websites we found in 2016 had a CAPTCHA service. But automated programs could respond to the kinds of CAPTCHAs found on all the state websites that had CAPTCHAs, thereby rendering them a nominal deterrent. Improvements have been made in recent CAPTCHAs.

My colleagues and I urge the Subcommittees to explore ways to help state and county websites use special codes that may appear on driver licenses and to use the latest versions of CAPTCHAs on websites that allow voters to change voter information.

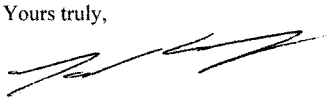
My colleagues and I also urge the Subcommittees to provide research funds to develop anomaly detection algorithms on voter data so that unusual activity can be identified, and alerts sent to officials for human inspection. These alerts can identify an assortment of problems, even violations that come from penetration of the perimeter security. (In the interest of full disclosure, my colleagues and I have begun such an effort.)

I also want to make a distinction that the websites having the vulnerabilities we describe are websites that allow voters to change their voter information. Sometimes, these were voter registration websites, but other times, they were motor vehicle websites that did not even allow new voters to register to vote but did allow voters to change existing registrations.

My colleagues and I are busily re-surveying the state websites now to provide updated information. When these results are finalized, we will forward them to you.

I ask that this letter be entered in the hearing record. My colleagues and I look forward to working with the Subcommittees on these issues of vital importance to the American public.

Yours truly,



Latanya Sweeney, PhD.

Latanya Sweeney PhD is Professor of Government and Technology in Residence at Harvard's Department of Government and the founding Director of Data Privacy Lab at the Institute for Quantitative Social Science. Sweeney creates and uses technology to assess and solve societal, political and governance problems, and teaches others how to do the same. She pioneered the field known as data privacy and her work is cited in the HIPAA Privacy Rule and other federal privacy regulations worldwide. Her work on discrimination in online ads ignited the new research area known as algorithmic fairness. She is an elected fellow of the American College of Medical Informatics, with more than 100 academic publications, 3 patents, and 3 company spin-offs. She has received numerous professional and academic awards and testified before federal and international government bodies. Among other federal appointments, Sweeney formerly served as the Chief Technology Officer at the U.S. Federal Trade Commission.

In 2018, Harvard launched its new Program in Technology Science, which prepares students for jobs as technologists that work in the public interest. The program is based on Sweeney's prior success at teaching students to scientifically assess unforeseen consequences in technology and to work in civil society organizations, government, and technology companies. Sweeney joined with 50 scholars worldwide to launch the Technology Science Initiative to promote the approach broadly.

Sweeney earned her Ph.D. in computer science from MIT in 2001, being the first black woman to do so. Before joining Harvard as a faculty member, Sweeney was the Distinguished Professor of Computer Science and Policy at Carnegie Mellon University, where she taught computer science, technology and policy from 1998 to 2011. She currently serves as the X.D. and Nancy Yang Faculty Dean of Currier House at Harvard College. Beginning next month, she will also serve as a member of the inaugural global Technology Policy Council of the Association for Computing Machinery, the world's largest association of computer scientists and professionals. More information about Professor Sweeney is available at her website (http://latanyasweeney.org/).

Chairwoman SHERRILL. Thank you. Mr. Ziriax?

TESTIMONY OF MR. PAUL ZIRIAX,
SECRETARY, OKLAHOMA STATE ELECTION BOARD

Mr. ZIRIAX. Thank you very much. And I do want to thank my representative, Ms. Horn, for the kind introduction. I am her constituent, so I think that's a prerequisite when here, but thank you very much for that. I also want to thank the full Committee Ranking Member, Mr. Lucas, who is also from Oklahoma, who ensured my invitation here today. So, Chairwomen Sherrill and Stevens, and Ranking Members Norman and Baird, also Chairwoman Johnson of the full Committee, and distinguished Members of the Subcommittees, I want to thank you for the opportunity to testify today. My name is Paul Ziriax. I'm the Secretary of the Oklahoma State Election Board, and the Chief State Election Official. Different from many States, Oklahoma has a voting system that is uniform, and Statewide, owned and controlled by the State Election Board. Our system utilizes paper ballots that are hand-marked by voters, and counted by accurate, reliable, precinct-based optical scanners. And no matter where you are in our State, voting is the same. We have the same style of ballots, the same voting hours, the same standards and regulations, and the same accurate optical scanners.

In my written testimony you can read much more about Oklahoma's election system and procedures, including our relatively low costs, the bipartisanship of the system, the—and the speed with which we are able to count ballots and certify results. In my opinion, Oklahoma's uniform system helps make it more secure, easier to maintain, more efficient, more cost effective, and more equitable to voters across our State. In my written testimony you can read about our—security features of the system, but we are very proud that our system is auditable and verifiable. At my request, my State legislature passed a new law this year that authorizes post-election audits beginning in 2020. But, as an election official, I do want to say, although I want to make voting and voter registration as convenient and as accessible as possible, we, as election administrators and policymakers, must be cautious about sacrificing too much security in the name of convenience.

I will say, in 2017, when I learned from Homeland Security that Oklahoma was unsuccessfully targeted—was one of the 21 States unsuccessfully—or at least we were unsuccessfully targeted, we have taken a number of steps to improve election security. For example, our systems are actively monitored and protected by our State Cyber Command. We joined several Federal and State agencies to create an election security working group to enhance communication and information sharing. We are members of the EI-ISAC, which is the election infrastructure information sharing network. We work closely with State Cyber Command, NASED (National Association of State Election Directors), and social media sites to help protect against misinformation campaigns, and our county election boards are now required to notify the State if physical intrusions or cyber incidents occur in their counties.

Now, speaking only for myself, I do want to offer some recommendations. The VVSG, which was mentioned earlier, should re-

main voluntary, and should contain broad-based goals that States can determine how best to implement. These standards, though, must be flexible so that they can adapt to changing threats and technology. Academia should work closely with current election administrators so that its recommendations are viable in the real world of election administration. All of us in this room should take great care so as not to unnecessarily alarm the public, or cause distrust in elections, especially when discussing theoretical threats without noting actual protections that exist against those threats.

Under our Federal system, the States should continue to administer elections in our country. I do not believe that election administration should be Federalized, and that—I believe that mandatory standards and certification procedures should not be forced on the States. The Federal Government should make technical assistance, best practices, voluntary standards, and intelligence available to the States. Sustained Federal funding for election security, or for upgrading voting systems, can be very helpful, but excessive mandates could cause States to refuse those Federal grants. When possible, I think intelligence regarding election security threats should be declassified quickly and shared with State and local election officials. And I do believe that every State should use voting systems that are auditable and verifiable, but that States should determine the best methods for auditing their elections.

In closing, my biggest concern as an election official is protecting the public's faith and confidence in the integrity of our elections. If citizens lose faith in our elections, then we risk losing our very representative republic. Physical security and cybersecurity are a great concern, but the easiest way to disrupt our elections, and what we've already observed, is for our adversaries to sow discord and spread misinformation. I encourage Federal policymakers to keep in mind that each State is different, and that imposing a one-size-fits-all mandate on the States for election policies or security procedures could be disruptive and expensive, and could unnecessarily create an adversarial relationship at a time when a cooperative partnership is needed. And, with that, I thank you for the time.

[The prepared statement of Mr. Ziriax follows:]

Testimony of Paul Ziriax

Secretary, Oklahoma State Election Board

Before the House Committee on Science, Space, and Technology
Subcommittee on Investigations and Oversight
Subcommittee on Research and Technology

June 25, 2019

Chairwoman Sherrill, Chairwoman Stevens, Ranking Member Norman, Ranking Member Baird, Chairwoman Johnson, Ranking Member Lucas, and distinguished Members of the Subcommittees:

Thank you for the opportunity to testify today. My name is Paul Ziriax. I am the Secretary of the Oklahoma State Election Board and the State of Oklahoma's chief election official, and have served in this capacity for more than a decade.

Established under the Constitution of the State of Oklahoma in 1907, the Oklahoma State Election Board is the administrative agency for the conduct of state elections and the oversight of the state's 77 county election boards.

Our mission statement is, "To achieve and maintain uniformity in the application, operation, and interpretation of the state and federal election laws with a maximum degree of correctness, impartiality, and efficiency."

In the early 1990s, the State of Oklahoma first implemented a uniform, statewide voting system using paper ballots that were hand-marked by voters and counted by accurate, reliable precinct-based optical scan tabulators.

Oklahoma was one of the last states to use its Help America Vote Act of 2002 (HAVA) funding to upgrade our voting system. The voting system in use today was deployed in 2012, and it continues our tradition of utilizing paper ballots that are hand-marked by voters and counted by accurate, reliable precinct-based optical scan tabulators. We believe we made the correct decision to use HAVA funds to stick with a paper-based, optical scan system.

The citizens of our state take great pride in our voting system. It is one of the most reliable, most accurate, most secure, most efficient, most cost-effective, and speediest voting systems in the entire world.

Representatives of both major political parties play a role in the administration of elections in Oklahoma – from our bipartisan county-level absentee voting boards, to our bipartisan pollworkers, to our bipartisan county election boards and State Election Board. Voters who are Independents or members of recognized minor political parties also serve as pollworkers.

In our state legislature, leaders and members of both major political parties trust the work we do at the State Election Board, and work with election officials to ensure that nonpartisan statutes and procedures are in place that instill public confidence in our state's election system.

We also run a lot of elections in our state. In odd-numbered years there are local elections every month except December. In Presidential election years, there are four state and federal elections in March, June, August and November, as well as local elections in January, February and April.

Although participation in early voting (officially known as "in-person absentee voting" in Oklahoma) and "no excuse" mail absentee voting has increased in recent years, Oklahomans still by-and-large vote on Election Day. While nationwide about 40 percent of voters voted before Election Day at the 2018 General Election, in Oklahoma more than 85% of votes were cast *on* Election Day.

OKLAHOMA'S UNIFORM STATEWIDE VOTING SYSTEM

Different from many states, Oklahoma's voting system is a truly uniform, truly statewide voting system.

No matter where you are in our state, voting is the same for the more than two million Oklahomans who are registered voters. Voters mark the same style of ballots, during the same hours, subject to the same standards and regulations, and tabulated by the same optical scanners.

The State Election Board owns the voting devices and election computers, owns the software used to program voting devices and tabulate votes, owns the voter registration system, and owns the network used to securely communicate with county election boards.

We do not contract out election programming or tabulation to private vendors. Our own State Election Board staff programs and tests every election database for every county for every election. County election board personnel use those databases to program voting devices, test ballots, and tabulate election results.

State Election Board staff conduct routine maintenance of voting devices annually, make most repairs to our voting equipment, and oversee major repairs that are covered by the manufacturer's warranty.

Prior to each election, state and county election officials conduct extensive pre-election testing of voting devices, software and ballots.

For every election, no matter how large or small, the State Election Board staff prepare the ballot files. All ballot printing vendors are certified and subject to the supervision of the State Election Board. The State Election Board contracts with printers for federal and state ballots, while each county election board has a contract printer for ballots for local elections.

Under Oklahoma state law, the Secretary of the State Election Board has direct supervisory authority over county election boards, and has the statutory responsibility to develop the election procedures and training used by county election boards. This helps to ensure that our state's uniform procedures and policies are followed.

It is my opinion that Oklahoma's uniform voting system helps to make our system more secure, easier to maintain, more efficient and cost effective, and more equitable to voters across our state.

* * * * * * *

In Oklahoma, our state laws require elections to be completed speedily.

At the November 2018 General Election, every ballot that was cast by mail, during early voting, and on Election Day was counted and the unofficial election results posted on our website by 10:30 p.m. on Election Day. That's every vote out of nearly 1.2 million ballots cast for Governor and eight other statewide officers, U.S. Representative, both houses of the State Legislature, district judge and associate district judge, district attorney, numerous county officers, retention races for four

Supreme Court justices and eight appellate judges, and five state questions, and even local offices.

By 2:00 p.m. on the Friday following the General Election nearly 1,200 provisional ballots statewide were approved by county election boards for counting. Three hours later, at 5:00 p.m., those provisional votes were added to the vote totals and final results were certified by the 77 county election boards.

At 5:00 p.m. on Tuesday, November 13 – just one week after the 2018 General Election – the State Election Board officially certified the results of all state and federal elections and the State Election Board Secretary issued official certificates of election to all state and federal candidates for office. Members of the Oklahoma State Legislature officially took office a week later.

Oklahoma's voting devices are known and trusted in our state for their accuracy. While hand recounts are occasionally requested by candidates, the initial outcome of an election has not been changed as the result of a recount.

I believe the speed with which Oklahoma election officials are able and required to tabulate and certify results helps instill confidence in our system.

* * * * * * *

Because of our system's efficiencies, we are able to conduct elections relatively inexpensively in Oklahoma. For example, the State Election Board expended a *total* of $3.4 million to conduct three statewide elections in 2018 (Primary, Runoff Primary, and General Elections), and another $546,000 on election supplies, overtime, and training for the entire 2018 election cycle. Most of the 77 county election boards have extremely limited budgets, and we estimate that they spent less than $900,000 *combined* to conduct the 2018 General Election.

Our State Election Board staff consists of 23 full-time and 2 part-time personnel. Most county election boards are staffed by the secretary and one assistant. (The largest at any county election board is Tulsa County, which currently has 19 fulltime personnel.)

The efficiency of Oklahoma's voting system is by design. Dates and deadlines are staggered so that the limited number of state and county personnel can complete one set of tasks, and then move on to the next. For example, prior to the voter registration deadline county election boards can focus on processing voter

registration applications. They then move on to processing absentee ballot applications, and after the absentee ballot request deadline the early voting period begins. After the early voting period ends, they can process incoming mail absentee ballots and finalize preparations for Election Day.

These specific stages of Oklahoma's election process allow our state and county election staff to accomplish a great deal with limited funds and limited staff, yet with a maximum amount of security and accuracy.

* * * * * * *

In Oklahoma we have made significant improvements in services to voters in recent years.

- **Online Voter Registration Updates**: In 2018 we launched the first phase of our online voter registration system, which allows registered voters to update their addresses and party affiliations online. Though submitted electronically, these updates must be processed and approved individually by county election board personnel. Foreign IP addresses are automatically blocked from using this system, and election officials and the state cyber command monitor the system and its logs.

- **Oklahoma Election Results (OKER)**: Also in 2018, Oklahoma launched an enhanced, accessible election results platform that allows end-users to receive real-time election results in a variety of formats for every race down to the precinct level. These results, however, are not the official results, and if the public platform were to go down, the election results themselves would not be impacted.

- **Oklahoma Military and Overseas Ballots Online (OMOBO)**: To comply with the Military and Overseas Voter Empowerment (MOVE) Act, the State Election Board developed this module to securely deliver absentee ballots and materials to UOCAVA-eligible voters who request it. (For security reasons, voted absentee ballots must be returned by traditional means, not electronically.)

- **Online Voter Information Request System (VIRS)**: This system allows authorized users to download publicly available voter registration lists. Only

information required to be made public under Oklahoma's Open Records Act is available through this system.

- **Online Voter Tool (OVT)**: Voters can confirm their registration, find their polling place, track the status of their absentee ballot, check the status of a provisional ballot, and view a sample ballot for their precinct.

- **Online Absentee Ballot Application**: A registered voter may use this portal to electronically apply for an absentee ballot. Though submitted electronically, these requests must be processed and approved individually by county election board personnel. Like voter registration updates, election officials monitor logs and other back-end activity.

- **Electronic Voter Notifications**: Voters can sign up to receive notifications by email or text message about elections that are scheduled in their county, voter registration deadlines, absentee ballot request deadlines and more. This helps election officials directly communicate with voters, reducing the risk of misinformation being distributed.

- **eScan A/T with Audio Tactile Interface (ATI)**: Each precinct-based optical scanner is equipped with an Audio Tactile Interface (ATI) for use by voters with disabilities so they can vote privately and independently. A paper ballot is used to activate an ATI session, at which time a voter casts votes using an audio version of the ballot. Voters may use the provided interface or a variety of other tools, such as a sip-and-puff or paddle interface. An ATI voter receives an audio confirmation of his or her votes prior to casting the ballot.

There are many more improvements for voters that are currently in development in Oklahoma:

- **Oklahoma Voter Services Portal (OVSP)**: This is a "one-stop-shop" that will bring several current individual services into a single enhanced application. It will allow voters to confirm their voter registration, update their voter registration address or party affiliation, apply for an absentee ballot, track the status of an absentee ballot, find their polling place, view a sample ballot for their precinct, check the status of a provisional ballot, find contact information for their county election board, and more.

- **Precinct-based Electronic Voter Check-in**: Oklahoma currently uses paper-based pollbooks. This system would allow voters to check in electronically at their polling place. Paper pollbooks will continue to be available as a backup.

- **Online Voter Registration**: When fully implemented, Oklahoma's online voter registration system will allow citizens to register to vote for the first time, transfer their registration to another county, and make updates to the current voter registration. For security reasons, the system will be required to confirm that an applicant's information matches the information on their Oklahoma driver license or Oklahoma state identification. All activity will be monitored on the back-end by election officials for anomalies.

SECURITY OF OKLAHOMA'S ELECTION SYSTEM

In Oklahoma we take seriously the need to protect the security and integrity of our elections. Here are some examples, though not an exhaustive list, of how we protect elections in Oklahoma.

- Oklahoma uses paper ballots and our system is auditable and verifiable. We conduct extensive pre-election testing of voting devices, software and ballots at both the state and county level, and a new law enacted this year authorizes post-election audits beginning in 2020.

- Oklahoma's voting devices, voting system software, computers used to program voting devices, and computers used to tabulate results are never connected to the Internet.

- The voting system has numerous built-in safeguards. For example, if any part of the system is tampered with – from the tabulation computer to the voting device to the ballots – it is designed to "break" and will fail to work with the system's other components.

- Although we have a "uniform" election system, the various system components and applications are contained within their own silo so that an incident in one does not spread to the others.

- Network connections with county election boards are secured and require multi-factor authentication. The voting system, election management system, and voter registration system require multiple layers of authentication.

- We maintain a strict chain of custody for voting devices and ballots, from before an election until that election is certified.

- Members of both major political parties are required to be members of absentee voting boards, precinct voting boards, county election boards, and the State Election Board.

- Candidates in any race can contest the results of an election by requesting a recount or by filing a petition alleging election irregularities.

- To utilize online services, such as updating a voter registration or requesting an absentee ballot, a voter must confirm his or her identity prior to being allowed to use the service. Though submitted electronically, updates and requests using these online services must be processed and approved individually by county election board personnel.

- The identity of an absentee voter is confirmed prior to the submission of a voted absentee ballot through the notarization or witnessing of an absentee ballot affidavit.

- Our statewide system makes it much easier to secure at the state level than having to secure different systems at all the counties separately.

- Additional security improvements are described in the next section of this testimony.

As Oklahoma's chief election official, I want to make voting and voter registration as convenient and accessible as possible. However, I know we must seek the proper balance between convenience and accessibility on the one hand, and election security and integrity on the other. Election administrators and policy makers must be cautious about sacrificing too much security in the name of convenience.

STATE AND FEDERAL COOPERATION

Under our Constitution and federal system, election administration is and should be the responsibility of the states. However, given the potential threats to our elections, there is an important support role federal officials should play.

I was skeptical in January of 2017 when then-Homeland Security Secretary Jeh Johnson announced that election systems would be added to the list of the nation's critical infrastructure. This skepticism was largely due to the lack of information provided to me as an election administrator.

However, things began to change when I was told by Homeland Security in 2017 that Oklahoma had been one of 21 states "targeted" in 2016. The good news for my state is that these probes were not successful, and were not direct probes of our state's election or voter registration systems, but rather to the broader state government network. This brought home to me the need for additional cooperation and communication between the State Election Board and federal and state security and intelligence officials.

Since that time we have taken a number of steps in Oklahoma to improve election security.

Our election systems are actively monitored and protected by the state cyber command. We are members of the ISAC. We have created a partnership with numerous federal and state agencies as part of an election security working group.

We work closely with NASED and social media companies to help protect against misinformation campaigns. For major elections, our state cyber command monitors social media and alerts election officials to any possible issues.

Under a new state law, county election boards are required to notify the State Election Board if physical intrusions or cyber incidents occur.

State election officials are working with the state cyber command and state security officials to further enhance cyber security and physical security for our elections.

Our election security working group has grown to include officials from the State Election Board, U.S. Department of Homeland Security, Oklahoma Office of

Homeland Security, Oklahoma Cyber Command, Oklahoma Department of Emergency Management, Oklahoma National Guard, and the FBI.

This group took steps in advance of the 2018 elections to enhance communication and information sharing among our various agencies. We met regularly to discuss risks and plan for contingencies. We arranged for unclassified briefings and security training for county election officials, and shared "best practices" with state and county election employees.

I want to take a moment to commend the U.S. Department of Homeland Security for reaching out to me and expediting a security clearance so relevant intelligence related to election security can be shared as needed. I also cannot say enough good things about the local DHS officials in Oklahoma, as well as the FBI field office, and how helpful they have been in their efforts to share intelligence and services.

RECOMMENDATIONS

Speaking only for myself as Oklahoma's chief election official, I offer the following recommendations to policy makers, federal agency personnel, academia, and other interested stakeholders:

- Oklahoma's representatives on the EAC Standards Board have advised me that NIST and the EAC are making significant progress with the development of VVSG 2.0. To be successful and to encourage maximum cooperation by state and local election officials, the VVSG must remain voluntary and should contain broad-based goals that states can determine how best to implement. These standards also must be flexible to adapt to changing threats and technology.

- When developing proposals for election administration or election security, academia should work closely with current election administrators so that recommendations are viable in the real world of elections. The National Academies made some good recommendations in 2018, for example, but not all are viable or applicable in every jurisdiction.

- When conducting hearings, performing studies or releasing recommendations, academia, policy makers and others should take great care so as not to unnecessarily alarm the public and cause distrust in

America's elections. This is especially true when discussing "theoretical" threats while failing to note real world protections against such threats.

- Under our federal system, the states must continue to administer elections in this country. Election administration should not be federalized, nor should mandatory federal standards and certification procedures be forced on the states.

- The federal government should make technical assistance, best practices, voluntary standards, and intelligence available to states.

- Continue to expand and improve communication between federal agencies and state election officials.

- Additional federal funding for election security or for upgrading election systems could be helpful, provided that it is sustained and not one-time only. However, if too many conditions or mandates are required to receive such funding, many states may refuse to accept federal grants.

- When possible, intelligence regarding election security threats should be declassified quickly and shared broadly with state and local election officials.

- Federal and state security officials should promote election security awareness with election officials and the public.

- Federal and state officials should continue to work continue together to improve public confidence in America's electoral system.

- States should use voting systems that are auditable and verifiable, but states should be the ones to determine the best methods for auditing their elections.

IN CLOSING

My biggest concern as an election official is protecting the public's faith and confidence in our elections. If citizens begin to lose faith in the accuracy and validity of vote counts, then we risk our very representative republic itself.

With that in mind, I believe the potential for the spread of misinformation about election policies and procedures through social media or other means is likely the most serious near-term threat. Physical security and cyber security are also a concern, but the easiest way to disrupt our elections – and what we have already observed – is for our adversaries to sow discord and spread misinformation.

I encourage federal policy makers to keep in mind that each state is different. Imposing "one size fits all" mandates on the states for election policies or election security procedures will be disruptive and expensive, will risk setting up state and local election officials for failure, and will likely create an adversarial relationship at a time when a cooperative partnership is needed.

Oklahoma election officials know more about running elections in our state than a federal employee in Washington or an out-of-state college professor ever could. Laying out broad-based goals and best practices – and allowing states to determine how to meet these goals – is the best way to proceed.

# # # #

Paul Ziriax

Biography



Paul Ziriax (pronounced ZEER'-iks) has served as Secretary of the Oklahoma State Election Board since 2009 and is Oklahoma's chief election official.

He is also the Secretary of the Oklahoma State Senate. (Since 1913, Oklahoma law has required the Secretary of the State Senate to serve as the Secretary of the State Election Board.)

Originally from Claremore, Oklahoma, he has worked as a senior aide in the Oklahoma State Senate, as chief of staff and press secretary to a Member of Congress from Oklahoma, and as a radio station music director and announcer.

Ziriax is a member of the National Association of State Election Directors and the American Society of Legislative Clerks and Secretaries, and is a past appointee to the Oklahoma Capitol Preservation Commission. He is an alumnus of Oklahoma State University in Stillwater.

Chairwoman SHERRILL. Thank you. Dr. Benaloh?

TESTIMONY OF DR. JOSH BENALOH,
SENIOR CRYPTOGRAPHER, MICROSOFT RESEARCH

Dr. BENALOH. Thank you, and good afternoon Chairs, Ranking Members, other Members of the Subcommittees. I very much appreciate the opportunity to speak before you this afternoon. My name is Josh Benaloh. I'm Senior Cryptographer at Microsoft Research. My 1987 doctoral dissertation at Yale University was entitled "Verifiable Secret Ballot Elections", so I've been working on election technologies for an embarrassingly long time. I also had the privilege and pleasure of serving alongside Neal Kelley on the National Academies' recent report on securing the vote, and appreciate that experience as well.

There are thousands of election jurisdictions in the U.S., over 8,000 by most counts, and most are very small, with very limited resources. Threats come from nation-state sponsored adversaries, in many cases. This is an asymmetric battle. And while we have certainly a responsibility to harden our election infrastructure to the extent that we can, we should recognize that we cannot realistically make our election infrastructure impervious to attack. While we cannot guarantee that attacks can be prevented, we can guarantee that they're detectable. And the National Academies' report recommends pursuing two technologies that enable auditing that enables us to detect any attacks on our infrastructure. One is called risk-limiting auditing, the other is end-to-end verifiability.

Risk-limiting audits are an enhanced form of traditional audits, managed by, and overseen by election officials, ideally together with, in cooperation with, members of the public. They use advanced statistical methods to make the auditing process more effective and more efficient, and they have been piloted in many jurisdictions—probably about a dozen jurisdictions around the U.S. in recent years. End-to-end verifiability is something entirely different. It's a public means of auditing. It's a method that allows any individual, after an election closes, at any time to conduct an audit. There's no need to wait for election officials, for Judges to issue court orders. Candidates, members of the news media, interest groups, and even individual voters can check for themselves that the votes have been counted correctly. Any and all tampering can be detected. Not just external tampering, but even insider tampering, due to faulty equipment, or improper actions by election personnel.

End-to-end verifiability effectively answers the question, how can I trust the results of an election when I don't trust the people or equipment on which the election has been run? This is not a new technology. It has actually been around for decades. Its seeds go back to the 1980s, but it has evolved during that time, and improved, and become more efficient, and more practical, and more friendly, and is ready for wide-scale deployment at a time when I believe we most need it.

Just over a year ago, Microsoft announced its Defending Democracy program, and as part of that, just last month Microsoft announced its ElectionGuard system. Microsoft is working with partners, including Columbia University, and a Portland company

called Galois to build a free, open-source, software toolkit that enables both end-to-end verifiability and risk-limiting audits. This is not intended to replace existing systems for counting votes. It goes alongside. It makes it possible to have an auxiliary verifiable count that is verifiable by anybody at all. We are working with many vendors to promote the adoption of this technology, and seeking jurisdictions for initial pilots. The technical details will be released shortly, and the toolkit that enables this will be available later this summer.

There are, however, regulatory challenges to making this happen, and the NIST and EAC guidelines that are in existence today are somewhat old and dated. They don't recognize new technologies, they're not very flexible, so we very strongly support and encourage the adoption of the new VVSG 2.0 Guidelines that are in draft form, and hope they will be adopted very soon.

There are numerous other challenges facing our election infrastructure: Technical, financial, educational, and others. Congress, in collaboration with States, can help to provide consistent funding sources, and address many of the challenges we face. Thank you very much, and I look forward to your questions.

[The prepared statement of Dr. Benaloh follows:]

Written Testimony of
Josh Benaloh

Senior Cryptographer
Microsoft Research
Microsoft Corporation

to the Subcommittee on Investigations & Oversight
and the Subcommittee on Research & Technology
of the House Committee on Science, Space, & Technology
to review Election Security: Voting Technology Vulnerabilities.

June 25, 2019

Chair Sherrill, Chair Stevens, Ranking Member Norman, Ranking Member Baird, and Members of the Committees, thank you for the opportunity to testify about the important issue of deploying technology to improve the security of U.S. elections.

My name is Josh Benaloh, I am the Senior Cryptographer at Microsoft Research[1]. Microsoft's research operations span 17 locations worldwide, employing well over 2,000 people conducting research and advanced development in computer science, electrical engineering, economics, physics, biology, and social science. These research operations are embedded in R&D operations across Microsoft that represent an annual investment of over $14 billion.

In addition to my position at Microsoft, I hold an Affiliate Faculty position in the Paul G. Allen School of Computer Science and Engineering at the University of Washington. I earned a degree in Mathematics from MIT and M.S., M.Phil., and PhD. Degrees in Computer Science from Yale University, where my 1987 doctoral dissertation was entitled "Verifiable Secret-Ballot Elections." I have spent the last 30 years working on the complex and intricate problems of election security and integrity.

[1]Microsoft Research, https://research.microsoft.com/

When individuals cast their ballots in a free and fair election, they experience democracy in its most personal form. They select leaders and provide direction for their communities, and in the United States they do so within the privileged protection of a secret ballot. When adversaries attempted to interfere in the 2016 U.S. elections their actions threatened more than just the integrity of the vote itself; they threatened to undermine our collective faith in the entire electoral process.

Building and maintaining voter confidence in elections is a multi-facetted task that cannot be accomplished by one organization or entity alone. Microsoft believes it will take extensive effort from the Federal government, state and local governments, election system vendors, the technology sector, academia, civil society, and voters themselves to come together and drive solutions.

For that reason, last year Microsoft formed the Defending Democracy Program, which works with a variety of governmental and non-governmental stakeholders in democratic countries globally to achieve the following goals: [2]

- **Protect campaigns from hacking** through increased cyber resilience measures, accessible and affordable security tools, and incident response capabilities;
- Explore technological solutions to **preserve and protect electoral processes** and engage with federal, state, and local officials to identify and remediate cyber threats; and
- **Defend against disinformation campaigns** in partnership with leading academic institutions and think tanks dedicated to countering state-sponsored computational propaganda and junk news.

National Academies Report

Recently, I had the privilege and pleasure of serving on the National Academies of Science, Engineering, and Medicine committee on the Future of Voting which spent nearly two years gathering and synthesizing information. The committee's

[2] "Defending Democracy Program", https://news.microsoft.com/on-the-issues/topic/defending-democracy-program/

report – "Securing the Vote: Protecting American Democracy" – was published in September of 2018[3].

The report included numerous findings and 41 specific recommendations, and it devoted an entire chapter to election integrity. With regard to cybersecurity, the report noted the asymmetric relationship between the thousands of electoral jurisdictions in the United States – most of which are very small – and the potential nation-state level attackers who may threaten these jurisdictions. The report concluded that the diversity of the U.S. election infrastructure weakens – rather than strengthens – the security of our elections, and that although we have a responsibility to apply best practices and try to harden our electoral infrastructure, it is simply not reasonable to think that we can make our infrastructure impervious to attack.

Instead, the report noted the importance of auditing technologies that can detect compromises of our election systems – even if attacks cannot always be prevented. The report specifically recommends pursuing both **risk-limiting audits** and **end-to-end verifiability** as auditing technologies that can improve election integrity by enabling detection of any alteration of votes or tallies.

Risk Limiting Audits

Risk Limiting Audits (RLAs) are like traditional audits in that auditors – ideally together with members of the public – randomly select ballots and check to see that they are consistent with published tallies and other public data. Unlike traditional audits, however, RLAs use sophisticated statistical methods to dynamically determine the point at which an audit can conclude to achieve a pre-set level of confidence in the correctness of election results. RLAs can be far more effective and efficient than traditional administrative audits, especially when performed by comparing individual ballots against digital records of ballot contents.

RLAs have been piloted in several states and local jurisdictions, and some states have passed laws to require their use.

End-to-End Verifiable Elections

[3]Securing the Vote, https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

End-to-end verifiability offers a public means of auditing elections. Election administrators don't need to be trusted to follow correct procedures, and election equipment doesn't need to be trusted to function properly.

An election is *end-to-end verifiable (E2E)* if two properties are met.

1. Voters can verify the accurate recording of their votes, and
2. Anyone can verify the accurate tallying of the recorded votes.

In other words, in an E2E-verifiable election, any alteration or incorrect counting of votes in an election can be detected by candidates, political parties, news outlets, interest groups, and even voters themselves; and this capability extends not only to external threats but even to potential internal threats by faulty or malicious equipment and by careless or dishonest election officials.

The technologies that enable E2E-verifiability are not new – they date back more than 30 years. However, they have evolved over that time and have become more practical, efficient, and voter friendly. After years of academic research and small pilots, the technology is now sufficiently mature and stable for widespread public use.

ElectionGuard

Microsoft is working to advance the development and adoption of E2E-verifiability and RLAs. Later this summer, along with partners, Microsoft will make available an open-source software developer kit (SDK) called **ElectionGuard** which will be available on GitHub for anyone to access freely. This software will enable voting system vendors, existing as well as new, to build end-to-end verifiability into their systems.

The technology is intended to augment – rather than replace – existing voting systems. It can be used in conjunction with a variety of voting scenarios including electronic ballot marking devices and hand-marked paper ballots read by precinct-based optical scanners. The voting processes will be almost identical to the processes that voters use and are familiar with today - with one exception. Voters will receive and be able to leave their polling locations with printed tracking codes and instructions for how they can, if they choose, confirm their votes when the election closes.

Ballot privacy is critical in elections. Elections have the unusual, perhaps even unique, requirement of not allowing participants to reveal their data – even if they choose to do so. A voter who can reveal a vote to someone else can sell that vote or be coerced into voting according to the wishes of another. Even though voters can verify the accurate recording of their votes, they cannot use their tracking codes to reveal their votes, and their privacy is thus protected.

ElectionGuard will enable election officials to publish encryptions of all votes cast in an election. Voters will have the ability to use their unique tracking codes to look up their encrypted votes and confirm that they are unaltered and correctly counted, but these tracking codes neither reveal votes nor allow them to be shown to others.

Microsoft will publish an open specification in conjunction with ElectionGuard that will enable anyone to write an election verifier that can review an election record and confirm that the encrypted votes are all properly constructed and correctly tallied. This will enable news outlets, universities, civil society organizations, candidates, political parties, and even individual voters to build their own programs to verify the results of an election. This confirmation is based entirely on the publicly available election record that is produced by an E2E-verifiable system and requires no special access nor trust in the system that produced the public record. Anyone can then run verifiers built by organizations or individuals they trust to publicly confirm that the results of an election are accurate.

In addition to enabling E2E-verifiability, the ElectionGuard SDK can enable an enhanced form of risk-limiting audits (RLAs) that offers better privacy than the systems in current use. At present, the process for implementing the highest quality RLAs includes the publication of digital cast vote records (CVRs) corresponding to the physical ballots cast in an election. However, the publication of these CVRs can subject voters to coercion and allow them to sell their votes. By using the ElectionGuard SDK, election officials will be able to publish CVRs in an encrypted form that doesn't impede auditing and allows for public verification of the election tallies – all without releasing sensitive raw election data that can be abused by malicious actors.

Together with the ElectionGuard SDK and specification details, Microsoft is working to produce reference implementations that demonstrate how the software can be effectively incorporated in a variety of settings. The first will be a universally-accessible ballot marking device designed to be easily usable by any voter – including those with a wide range of accessibility needs. An optical scanner that can support E2E-verifiability and enhanced RLAs with hand-marked paper ballots is also being designed. By providing tracking codes as a means of enabling verification of accurate recording of votes, the ElectionGuard SDK enables more accessible and usable voting methods with higher assurance than those in use today.

ElectionGuard and the associated reference implementations are the result of partnerships with many organizations, including Columbia University, Free&Fair, the Center for Civic Design, and VotingWorks.

System Certifications

For the sake of election security as well as ensuring a positive experience for voters, it is imperative to create an environment where innovation is possible. The current certification environment has significant limitations that can stifle the introduction of advanced technology into this market.

In 2002, the Help America Voting Act (HAVA) created the **Election Assistance Commission (EAC)** to set voting system standards, provide for the testing and certification of those voting systems, establish guidelines against which those systems are certified, and accredit independent non-federal laboratories that certify voting systems[4]. The EAC currently lists 57 certified voting systems deployed by seven registered voting system manufacturers.

The EAC certifies voting systems against the Voluntary Voting System Guidelines (VVSG). The EAC produced the first version of these guidelines, the 2002 Voting System Standards (VSS) prior to the enactment of HAVA. At that time, the VSS did not focus on security; but rather, "specif[ied] minimum functional requirements, performance characteristics, documentation requirements, and test evaluation criteria." There are currently 5 voting systems certified against these 2002 standards.

[4] 52 U.S.C. § 20971.

In 2005, the EAC updated the guidelines in collaboration with the Technical Guidelines Development Committee (TGDC) and the National Institute for Standards and Technology (NIST). These updated 2005 Voluntary Voting System Guidelines (VVSG 1.0) added security requirements to the certification criteria. The purpose of VVSG 1.0 was "to provide a set of specifications and requirements against which voting systems can be tested to determine if they provide all of the basic functionality, accessibility, and security capabilities required to ensure the integrity of voting systems." Of the 57 currently certified voting systems, 52 are certified against the VVSG 1.0. The EAC further modified the VVSG 1.0 and created the VVSG 1.1 to "enhance the testability and clarity of several of the requirements contained in version 1.0." No voting systems have ever been certified to VVSG 1.1; most systems in use were thus certified to a 2005 standard.

The certification process requires applicants to attest that the software submitted for certification testing shall be the exact software that will be used in production units consistent with section 1.6 of the VVSG 1.0. As the VVSG explains, "[t]o ensure that correct voting system software has been distributed without modification, the Guidelines include requirements for certified voting system software to be deposited in a national software repository. This provides an independent means for election officials to verify the software they purchase." This conformance requirement does not contemplate software updates, including security updates; and therefore, certified voting system software cannot be updated without losing its certification. This creates a dilemma for election officials when a vulnerability is discovered in a platform used by a voting system. The choice is between applying a security patch and losing certification or maintaining certification by using a system with a known vulnerability.

The EAC is now in the process of developing VVSG version 2 and has published the Technical Guidelines Development Committee recommendations – the VVSG 2.0 Principles and Guidelines document[5] – for comment. Notably, the Principles and Guidelines allows for software updates.

Microsoft has submitted comments on the VVSG 2.0 Principles and Guidelines. Those comments describe its strong support for the guidelines as an important step towards improving election technology security in the United States. Recognizing that diversity in organization, systems, networks, and assets of the

[5] VVSG 2.0 Guidelines, https://www.eac.gov/assets/1/6/TGDC_Recommended_VVSG2.0_P_Gs.pdf

elections infrastructure expands the attack surface and increases the risk of a cyber-attack altering elections results, Microsoft's comments specifically emphasize its support for the VVSG 2.0 guidelines on auditability. Microsoft hopes there is a speedy process that will result in more current technology in use in our elections.

Public/Private Partnerships

It takes engagement across sectors to secure our elections, which is in part why Microsoft opted to comment on VVSG 2.0. This kind of engagement and collaboration is key. Recently, there have been several examples of public/private engagements in election security that showcase progress.

Local Government Partnerships

Recognizing the need for improved collaboration among governors' offices, election officials, and state cabinet agencies within local jurisdictions across states, the National Governor's Association (NGA) recently established a policy academy to develop strategies to improve cybersecurity operations and communications around elections. Six states, including Minnesota, Idaho, Hawaii, Virginia, Arizona, and Nevada, will participate in this academy and receive cybersecurity technical assistance from the NGA. The NGA policy academy will run from June to December of this year. It is a partnership with the University of Southern California (USC) and supported by the National Association of State Election Directors (NASED) and the National Association of Secretaries of State (NASS), with financial support from the Democracy Fund.[6]

Microsoft understands the value of such local partnerships and the impact of private sector participation. For example, when Minnesota was seeking additional cybersecurity support heading into the 2018 elections, the Secretary of State reached out to Microsoft to form a partnership and quickly deploy solutions[7]. As announced in the press release:

[6] "States Get Assistance on Election Cybersecurity", https://www.nga.org/news/press-releases/states-get-assistance-on-election-cybersecurity/

[7] Minnesota press Release "Secretary Simon Announces New Steps To Enhance Election Cybersecurity," https://www.sos.state.mn.us/about-the-office/news-room/secretary-simon-announces-new-steps-to-enhance-election-cybersecurity/

"Outside forces are targeting for attack our instruments of democracy," said Secretary Simon. "In Minnesota, the stakes are particularly high because we are the #1 state in voter turnout – with a total turnout of 74.7% of eligible voters casting ballots in 2016. With the 2018 election rapidly approaching, I am grateful to Microsoft for working with my office to enhance and harden our election cybersecurity ahead of the 2018 General Election. This is one of many steps my office has taken to ensure that Minnesota is more prepared than ever before to confront outside threats to our elections."

Federal Government Partnerships

In January 2017, the U.S. Department of Homeland Security (DHS) designated Election Infrastructure as a critical infrastructure subsector of the Government Facilities critical infrastructure sector. Election Infrastructure typically includes both physical and digital components. Computers, servers, databases, and other information technology systems and assets are used to fulfill elections roles, including storing voter registration systems, managing the entire voting process, recording and tabulating votes, reporting election night results, providing the public with general elections information, and compiling and storing electronic poll books. Recognizing that many election infrastructure assets and systems are owned and operated by the private sector, this designation galvanized relationships between critical infrastructure owners and operators, state and local governments, and federal departments and agencies.

DHS led in this area by assisting private election industry owners and operators with forming an Election Infrastructure Subsector Coordinating Council (SCC)[8], where participants share and collaborate on issues of election security. Microsoft is pleased to participate in the Election Infrastructure SCC. DHS similarly established the Election Infrastructure Subsector Government Coordinating Council (GCC)[9], which brings together federal, state, and local government bodies, including the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED). DHS often brings both councils together to collaborate on cybersecurity strategies and plans.

[8]DHS Sector Coordinating Councils, https://www.dhs.gov/sites/default/files/publications/govt-facilities%20-EIS-scc-charter-2018-508.pdf

[9] https://www.dhs.gov/sites/default/files/publications/govt-facilities-election-infrastructure-subsector-gcc-charter-2017-508.pdf

In November 2018, DHS hosted a mid-term election day situation room. DHS recognized that a coordinated response from federal, state, local, and private sector groups is the best way to mitigate risks of malicious cyber-activity associated with elections. Microsoft was a participant and coordinated with Microsoft's own election day dedicated situation rooms in Washington, DC and Microsoft headquarters in Redmond, WA. Allowing elections infrastructure stakeholders to share information in real-time on election day facilitates a coordinated response should a cyber-incident occur.

Attempts to interfere with the electoral process extends to the political campaign environment as well, which has been very much in focus at the Federal Election Commission (FEC) this year. Though much attention has been given to the Russian "Internet Research Agency's" attempts to sow discord through online propaganda targeted at American voters, the hacking of the online accounts of political operatives and party committees must not be overlooked.[10]

With more than 60 million users of its paid Office365 (O365) cloud-based productivity software and free Outlook.com and Hotmail.com web-based e-mail services, Microsoft found itself in a unique position to protect election-sensitive users of its products against such hacking. To that end, Microsoft requested and received an advisory opinion from the FEC confirming that the company may offer a package of enhanced online account security protections at no additional charge on a nonpartisan basis to its election-sensitive customers, including but not limited to federal candidates and national party committees. The FEC concluded that the provision of AccountGuard[11] is permissible and is not a prohibited in-kind contribution under campaign finance law.[12]

Until this advisory opinion, the FEC had not robustly addressed the provision of cybersecurity services to political campaigns and national committees. In

---

[10]Ofc. of the Director of Nat' l Intelligence, Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections" (Jan. 6,2017) at 2-3, https://www.dni.gov/files/documents/ICA_2017_01.pdf; The John Podesta Emails Released by WikiLeaks, CBSNEWS.COM (Nov. 3,2016), https://www.cbsnews.com/news/the-john-podesta-emails-released-by-wikileaks/.

[11] "Protecting Democracy with Microsoft AccountGuard", (August 20, 2018), https://blogs.microsoft.com/on-the-issues/2018/08/20/protecting-democracy-with-microsoft-accountguard/

[12] FEC Advisory Opinion 2018-11, https://www.fec.gov/files/legal/aos/2018-11/2018-11.pdf

response, this advisory opinion sparked a series of similar requests for approval[13] from cybersecurity firms to provide cybersecurity services to members of Congress, political campaigns, and national committees.

These examples demonstrate that the private sector has a shared responsibility to protect the election ecosystem and we need the continued support and partnership of government counterparts at the local and federal level to do more.

Conclusion

As the 2020 election grows closer, it's clear that there is much work left to do. There are numerous challenges – technical, regulatory, financial, educational, and otherwise – to overcome. Congressional collaboration with the states to expedite and fund these efforts would help respond to these growing challenges.

I am encouraged to see organizations and individuals across many different sectors actively working together to identify solutions and drive improvement. The National Academies report offers numerous concrete steps which can dramatically improve the state of our election infrastructure. Microsoft's ElectionGuard and other offerings from its Defending Democracy Program can help address some of the technological challenges, but this represents only a fraction of the need. Congressional incentives to modernize our infrastructure and implement good auditing technologies together with work to update standards could help greatly at moving us towards a more secure election ecosystem.

I would again like to thank this committee for the opportunity to address this vital topic and look forward to your questions. Thank you.

[13] FEC Advisory Opinion 2018-15 (approving Senator Wyden's request to use campaign funds for cybersecurity expenses), https://www.fec.gov/data/legal/advisory-opinions/2018-15/; FEC Advisory Opinion 2018-12 (approving the provision of free cybersecurity resources to candidates and political party committees, by nonprofit corporation and its private sector sponsors and partners), https://www.fec.gov/files/legal/aos/2018-12/2018-12.pdf

Biography: Dr. Josh Benaloh

Josh Benaloh is Senior Cryptographer at Microsoft Research and an Affiliate Faculty Member of Computer Science and Engineering at the University of Washington. He earned his S.B. degree from the Massachusetts Institute of Technology and M.S., M.Phil., and Ph.D. degrees from Yale University where his 1987 doctoral dissertation "Verifiable Secret-Ballot Elections" introduced the use of homomorphic encryption as a means to allow individual voters to confirm that their votes have been correctly counted. Dr. Benaloh served seventeen years on the Board of Directors of the International Association for Cryptologic Research and currently serves on the Coordinating Committee of the Election Verification Network. He has been granted over fifty U.S. patents and has written and spoken extensively on cryptographic primitives and protocols, election technologies, and cryptographic policy. Dr. Benaloh is an author of the influential "Keys Under Doormats" expert report which details the damage that would be created by mandating exceptional government access to encrypted data. He is also an author of the U.S. Vote Foundation report on the viability of end-to-end verifiable Internet voting systems and recently completed service on the National Academies of Science, Engineering, and Medicine Committee on the Future of Voting whose final report "Securing the Vote – Protecting American Democracy" has been cited in numerous articles and deliberations.

Outside of professional activities, Dr. Benaloh served eight years on and chaired the Citizen Oversight Panel for Sound Transit which is investing $2 billion annually on expanding the public transit infrastructure for the Seattle region. He has also authored numerous puzzles for competitive puzzle-solving events.

Chairwoman SHERRILL. Well, thank you. Before we proceed, I would like to bring the Committee's attention to statements we have received from the Brennan Center for Justice, the Center for American Progress, and Verified Voting. We've also received letters to the Committee from the National Election Defense Coalition, and Common Cause. These documents highlight priorities that Members of this Committee should consider as we look to assist States in their election security efforts. Without objection, I will enter these documents into the record.

At this point we will begin our first round of questions, and I'll recognize myself 5 minutes.

So first I'd like to start, if I could, with Mr. Kelley. In 2018, my home State of New Jersey received a HAVA Election Security grant of nearly $9.8 million. So with this money, I'm happy to report we plan to purchase a number of voting systems that use a voter-verified paper trail audit, I'm sorry to report that New Jersey does not have that at this time, and to conduct a number of pilot programs with new systems. So what advice would you have for a State that decides to scale up their post-election audit pilots to a Statewide application?

Mr. KELLEY. Well, thank you, Madam Chair, for the question. I would have to go back to the discussion on risk-limiting audits, and, using that as really the benchmark for auditability post-election. In California we use two auditing functions right now. One is the 1-percent audit, which audits 1 percent of the precincts, the ballots that are cast within California, and then the second is the option of conducting a risk-limiting audit. Opening that up in a Statewide function, like we are in California, I think is the proper way to go, because it does give you that extra look and comfort at auditing functions post-election, when, even if you're manually counting the ballots, this gives you that extra added security and assurance that those audit—that the ballots are counted correctly.

So when you're looking at ramping up an auditing function, I think risk limiting audits is certainly the way to go. And there are so many States, and counties, and jurisdictions right now that don't utilize any auditing function, let alone a risk-limiting audit.

Chairwoman SHERRILL. Thank you very much. And, Dr. Sweeney, with the money we received, we're also making plans to allocate funds to implement any necessary changes to the Statewide voter registration systems. I know NIST and the National Academies have a lot of recommendations for how to do this. And, given your experience examining vulnerabilities in a broad swath of voter registration systems, what do you think are some of the most important first steps that New Jersey can pursue with these funds?

Dr. SWEENEY. Well, there's two sides. A lot of—my colleagues on the panel have really focused a lot on traditional—cybersecurity kinds of threats. Break-ins, ways that the data could be tampered with, changing the flow of the data. The example that I gave is not a break-in, it's the opposite. It's the—a fundamental problem we have in the United States about identifying citizens, or identifying Americans, or—and it's on—and how do we go about doing that when so much of the data on Americans is so publicly available?

And the study also gives us a hint at what was the best answer. Texas was the most difficult of the States, and it's because it used driver's license numbers, but it also used the number that was printed on the surface of the driver's license itself. It wasn't enough for us to stop the attack, but it limited—it raised the cost, because the only place you could get scans of actual driver's license to get those numbers was on the dark web. They weren't—that—those extra numbers weren't available elsewhere. So that gives us a sense of a way forward. Intrusion—and also intrusion detection would be helpful.

I would just say one more thing to New Jersey, and that is the idea of independent assessments are really important. If—we went through this with healthcare. If you build a system, and you say, this is what my security people say is good, and you test it, you're testing what you built it for. What we do is—and the reason you do independent assessment is the things you never thought of. It's a surface area you can't possibly think of. And the second part of that is whether or not New Jersey then—if a vulnerability is found, is—how robust is the response by New Jersey? We learned in the healthcare industry that if the hospitals just try to pretend it didn't happen to reassure everyone, that that's not nearly as good as a hospital who says, I had this vulnerability, we fixed it up, now we're ready to go. That kind of robust response is much more trustworthy. So I would recommend that approach.

Chairwoman SHERRILL. Thank you very much. And then, Dr. Romine, I have some straightforward questions for the record for you. Does NIST currently have the legal authority to develop technical guidelines for electronic poll books?

Dr. ROMINE. Thank you for the question. Under the *Help America Vote Act*, the work that we do with the EAC is constrained to voting systems, which are defined more narrowly. However, we do have a broad mandate for cybersecurity for a broader number of systems, and in the *COMPETES Act* (America Creating Opportunities to Meaningfully Promote Excellence in Technology, Education, and Science) we have more authorities there for cybersecurity in those systems.

Chairwoman SHERRILL. Thank you. And what about for voter registration databases and local election websites?

Dr. ROMINE. That would be the same answer. Not under HAVA, but under other authorities that we have, we could do work there.

Chairwoman SHERRILL. And same answer for election night reporting systems and ballot reconciliation methods?

Dr. ROMINE. That's correct.

Chairwoman SHERRILL. All right. Well, thank you very much. Thank you all. Now I'd like to, sorry, turn it over to Ranking Member Norman for 5 minutes.

Mr. NORMAN. Thank you, Chairwoman Sherrill. Secretary Ziriax, the substitute amendment to H.R. 2722 appears to contain several provisions that pertain to the administration of elections, as opposed to election security. To me, it appears that these election administration provisions are a Federal overreach that really encroach upon the function of State and local election administrators and their job. What are your thoughts about the bill? And, as an example, it looks like the bill requires paper ballots to be printed

on recycled paper produced in the United States. And is that your read of the bill, and what would a mandate like that mean for Oklahoma?

Mr. ZIRIAX. Well, in general let me say that when I was working with one of my home State Senators, and I apologize for mentioning a Member from the other body, but Mr. Lankford, when he was working on some election security, I told him many of the same things I'm about to tell you, that I do believe that it's important to remember the differences between different States. The recycled paper, for example, I personally—I—it is in the bill, I did read it there. I'm not exactly sure what the security purpose of that is. I know that with our current voting system, it cannot use recycled paper because of the sensitivity of the scanners, and what—if we were required to use recycled paper, it would actually run the risk of causing false readings.

Mr. NORMAN. Well, in your opinion, do you think the election administration provisions of the bill reach too far into the administration of elections, which really is inherently a function of each State?

Mr. ZIRIAX. I—in general, I think broad guidelines are better, and leaving specific decisions are better in the hands of the State.

Mr. NORMAN. OK. Mr. Kelley, you briefly discussed VVSG 2.0, and how it is structurally distinct from previous iterations of the VVSGs. Specifically, you indicated that the new structures aimed at providing high-level principles and guidelines on functions that are incorporated into devices that make up a voting system. From the perspective of State and local election officials, do you think the high-level approach taken by the VVSG 2.0 provides a more workable and implementable set of guidelines when compared to the previous iterations?

Mr. KELLEY. Yes, sir, thank you for the question. Actually, from the standpoint of security, reliability, usability, and accessibility, I definitely believe that. The principles and guidelines are high-level. They are certainly a good road map for heading down that path, but they're not in the weeds. They're not the test assertions, they're not the requirements. So, as it stands, those principles and guidelines in VVSG 2.0 I think are light years ahead, sir, of where we were.

Mr. NORMAN. OK. And, Secretary Ziriax, based on your experience, do you believe that a high-level approach is more workable and implementable, and is this the right approach?

Mr. ZIRIAX. That—in my opinion, yes. I'm very supportive of the VVSG 2.0 guidelines that are out there. Although I'm not speaking for the National Association of State Election Directors, NASED, I am a member, and I know that they have expressed concerns about a second part of that, where I know the EAC is seeking to vote on the actual testing standards. And, you know, my concern there is that, with the—with what we've seen in the past, with the lack of a quorum at the EAC, you run the risk then of getting stuck, as we currently are, with out-of-date standards.

Mr. NORMAN. Thank you. And, Dr. Romine, in layman's terms, can you describe what the election profile to the cybersecurity framework is, how it functions, and how it stands to help State and local election officials fortify their election systems?

Dr. ROMINE. Yes, sir. The cybersecurity framework that was spearheaded by NIST, and is now being adopted around the world, is a high-level document that is applicable and scalable to a wide variety of different sectors of the economy, for example. In order to be maximally useful to a specific sector, and in particular the critical infrastructure sectors that include the election infrastructure, certain tailoring needs to be done to the cybersecurity framework to make it maximally effective, and that's what we're actually working on right now. So it's essentially making sure that we make decisions that are predicated on the needs of a particular sector.

Mr. NORMAN. Great. Thank you so much. You all have been very responsive, and thank you for your questions. I yield back.

Chairwoman STEVENS. Thank you, Mr. Norman. The Chair will now recognize herself for 5 minutes of questions. And, certainly, we—we're capturing the nuance here, and how important the R&D is, and the trustworthiness, and the honesty, and the integrity of our election systems. I represent a suburban district in southeastern Michigan, and after the 2016 election, Michigan replaced its aging voting machines in basically every county in the State, spending $40 million in State and Federal money to do so, and it's one of at least four States, along with Florida, Illinois, and Wisconsin, that use cellular modems to transmit unofficial election results. And Michigan officials have said that the State's election machines are not connected to the Internet, eliminating a major hacking risk. Our Secretary of State, Jocelyn Benson, has implemented a Security of Elections Commission, a first of its kind commission. That's coming into formation this year. She's a newly won Secretary of State whose come in and put in that commission.

So Michigan voters are using paper ballots that run through an optical scan voting system, and, as we've noted, this week the House is considering H.R. 2722, *Securing America's Federal Elections Act*, which would require paper ballots and manual counting by hand or optical scanning systems, which is sort of a nice springboard to what we're doing here today, which is digging into the technology, talking about the R&D, relying on your expertise is a really robust panel. So—and there's obviously some, you know, ongoing debate about the use of modems and Internet connectivity in elements of the election system.

NIST has named this as one of its "open areas" still being considered in its ongoing efforts to update its Voluntary Voting System Guidelines. And so, Dr. Romine, can you just tell us where NIST is headed with this? Will NIST give us an affirmative finding about whether voting systems should avoid wireless and cellular modems, and minimize Internet connectivity?

Dr. ROMINE. Thank you, Madam Chairwoman. First I'd like to mention that the VVSG—the Guidelines that I've described are not solely NIST guidelines, but we're in partnership with the EAC, and with the TGDC, which is the advisory committee, so there's a number of people involved in the guideline development. But certainly in the Principles document in VVSG 2.0 we talk about some of the concerns regarding Internet connectivity, for example, actually, in VVSG 1.1 we talk about those concerns. We've had guidelines in the past, you talked about the paper ballots, about auditability. In the Guidelines that we put out, we're not specific on the way that

you can obtain auditability. We just try to ensure that auditability is available.

With regard to cellular modems, or any specific technology, we don't get into that level of detail, but we do talk a lot about the importance of Internet connectivity for voting systems as being a challenge to be managed.

Chairwoman STEVENS. Dr. Benaloh, would you say that—the general opinion of the computer science community, as to whether the risks of Internet connectivity and wireless access can be adequately mitigated?

Dr. BENALOH. I think the consensus is that—not at this time. There has been a good deal of exploration of use of Internet technologies associated with voting equipment, and there have been some studies looking at possibilities of how this might be done, and I believe the consensus is it would be premature to apply any of those technologies today.

Chairwoman STEVENS. Yes. And, Dr. Romine, you know, each fiscal year, NIST receives, you know, about the $1 to $2 million in appropriations transferred from the EAC budget to conduct its voting research, if I have that right, and testing, work required, you know, under HAVA, and these annual funds have been declined, even as needs have grown. How many NIST staff work on the NIST voting system project?

Dr. ROMINE. We have five Federal employees in my laboratory. Four of those are part time, one is full time, and then we have approximately four contractors working with them. That's the extent of our capacity currently to address these issues.

Chairwoman STEVENS. And, under those circumstances, how do you prioritize your voting technology efforts, given limited resources and constrained staffing?

Dr. ROMINE. Well, I'd like to point out that the activities that we have in cybersecurity are considerably larger than this one effort, and many of the activities—the research activities that we engage in are applicable in some ways to voting systems, and in particular to the more traditional systems, like the voter registration systems, which are much more similar to mainstream IT systems. So we do leverage a lot, and I'd just like to say we're very proud of what we do with the resources that we have.

Chairwoman STEVENS. We're proud of you, too. And we're also proud of your fabulous description of NIST in your opening testimony. We must have faith in our government, we must have courage, we must stick to our principles for the people, by the people. I don't even say bipartisan. I talk about the things that bring us together as a body. And, with that, I'm going to yield back, and I'm going to call on my fabulous colleague, Dr. Jim Baird, for his 5 minutes of questioning.

Mr. BAIRD. Thank you, Madam Chairwoman. Was that part of my time you were using? Dr. Romine, when you look at your knowledge, and your experience, and the number of times you've been here, maybe I should just allow you to decide what question you would like to answer. But I'm not going to do that. Here's a question. You know, in past testimony you mentioned the importance of collaboration with stakeholders in the realm of elections, and to be successful in creating voluntary standards. How often

does NIST meet with election officials, with industry, outside technical experts, and advocacy groups, and what's been produced as a result of these meetings, in your opinion?

Dr. ROMINE. Thank you for a question that allows me to brag about NIST a little more. I appreciate that very much. The subcommittee meetings I talked about, and the various task groups have meetings, virtual meetings, biweekly, in some cases weekly. The level of engagement is high, the amount of participation is high. The work that we're doing on the development of the Guidelines, and in the cybersecurity profile that I talked about, the cybersecurity framework profile, is a testament to the productivity of those activities. We work collaboratively with the Department of Homeland Security, and obviously with the EAC, in tackling some of these challenging issues with regard to security of many kinds, but security of our election systems in particular.

On the industry front, we have strong collaborations. One of the secrets of NIST is, because we're non-regulatory, I like to say aggressively non-regulatory, we have a very strong working relationship with industry in many, many different sectors of the economy, and certainly we have strong relationships with the election vendors as well.

Mr. BAIRD. Thank you. Dr. Ziriax, in your written testimony you described how efficient Oklahoma's election system is, and you state that the efficiency of Oklahoma's voting system is by design. How can we, at the Federal level of government, ensure that you get what you need to bolster the security of Oklahoma's election system without reducing the efficiency that your system has designed to achieve?

Mr. ZIRIAX. I'm very proud of our system, as I mentioned earlier. It's paper-based, it is auditable, it is verifiable. We use optical scanners. We have since the early 1990s. That's when we first developed our Statewide uniform system. In my opinion, the best thing that Congress can do is to help ensure that we have the resources from, you know, various Federal agencies for help. One of the things that I'm very proud of is the working relationship that we have with local, Federal, and State officials, Department of Homeland Security—both State and Federal—FBI, our State Cyber Command. They, and others, are all part of an election working group that we have, and I think making sure that those various entities and agencies have the resources to work with their local and State election officials is very important.

Mr. BAIRD. Thank you, and I have one more question for you. In your closing remarks, you said that the Federal policymakers should keep in mind that each State is different, and that imposing one-size-fits-all would be disruptive, expensive, and could create an adversarial relationship between State and local officials at a time when cooperation and partnership is very much needed. So how can we best help States improve the security of their election systems without encroaching on their Constitutional prerogatives, and at the same time ask any other things that you might consider important?

Mr. ZIRIAX. Well, thank you for the question. You know, Oklahoma is different from other States. My State has a little over two million registered voters. I believe Mr. Kelley's county has about

two million registered voters. I have counties in my State with fewer than 1,500 registered voters that are staffed by one county election board secretary and one staff person. And I think, you know, you have to keep in mind that, as you're looking at election legislation, the broader that you make any requirements, the more that you leave to local and State election officials to decide how to implement those, the better we can make it work for our States.

I know that—I believe in Oklahoma we know more how to run elections in our State than, you know, someone from Washington, D.C., or maybe a college professor from another State, for example.

Mr. BAIRD. Thank you, and I'm out of time, so I'm sorry I don't have questions for the other three of you, but thank you for being here.

Chairwoman STEVENS. Thank you, and the Chair now recognizes Mr. Tonko for 5 minutes of questioning.

Mr. TONKO. Thank you, Madam Chairwoman, and thank you for holding this hearing, and thank you to our witnesses for joining us. Election security goes to the very heart of America's ideal of government, of the people, by the people, and for the people. We need look no further for evidence of this fact than the widespread, well-documented, and ongoing attacks of America's adversaries on our election systems. Our enemies recognize the power of our elections, and we must do the same.

Today is Primary Day in the State of New York, and I am reassured that New York State has been taking election security seriously. I'm deeply concerned about the U.S. intelligence reports that 21 State election systems were targeted by Russian hackers during the 2016 election cycle. I agree with Special Counsel Mueller that all Americans should be concerned about the multiple systematic efforts to interfere in our election. This must be a wakeup call for all of us.

Assuring the principle of one person, one vote requires balancing security and accessibility. In developing election technology, it is crucial that the technology be both secure and accessible for blind Americans, for people with other disabilities that can make it harder to vote. In election infrastructure, there may be places where security and accessibility seem to compete with one another.

So, Mr. Kelley, is this the case? Are there places where the needs of blind voters, or voters with disabilities, are at odds with some of the efforts that have been undertaken to modernize election infrastructure?

Mr. KELLEY. Thank you, sir, for the question, and I think at times in the past that was the case. I think with technology, and where we are today, we do have the capability to produce paper ballots that can be used by voters with disabilities, and can be verified by voters with disabilities. And I would say the one area where they probably still intersect which is a little bit difficult is the remote transmission of ballots to individuals who are voters with disabilities. That's an area of concern that I think we need to keep an eye on, and security's very important in that regard. But I agree with you, sir, we can't lose sight of making sure that it's accessible at the same time.

Mr. TONKO. So that technology gap that you just identified, is that resolvable, or——

Mr. KELLEY. I believe it is. I think we're at a point now where we can transmit the ballot directly to that voter, it can be verified, and marked, and printed out, and then mailed back, so there's no transmission of that ballot over the Internet, or over any network. So I do think it's solvable, yes, sir.

Mr. TONKO. Thank you. And, Dr. Benaloh, did I say that correctly?

Dr. BENALOH. It's Benaloh.

Mr. TONKO. Benaloh, thank you. Based on Microsoft's work with election officials, what do you believe is the current cybersecurity posture and readiness of the average State election office, and is there even an average, or any—or are things all over the place?

Dr. BENALOH. I think it would be hard to define an average of any kind. States are—and local jurisdictions are certainly working to try to improve things, but there is certainly a lot more that can be done, and we are hoping that, with consistent funding, new technologies, new—a new regulatory environment we'll be able to enact better systems, with better technologies, that can better protect the American voter.

Mr. TONKO. And, Mr. Ziriax, what are the election security concerns that keep you up at night going into 2020?

Mr. ZIRIAX. When I'm—there are really three potential threats that we face. One is misinformation. That has happened. I think it continues to happen. Obviously cyber intrusions. And I haven't heard anyone yet today mention physical security. You know, you could have physical security threats at polling places, or at election offices, but all three of those things are things that we should be concerned about, and, in my opinion, should work together—State and Federal officials finding common ground about how to move forward.

Mr. TONKO. Thank you. And, Mr. Kelley, what about you?

Mr. KELLEY. I would just add to that, I definitely agree with what he's saying. Cyber, physical, but I would also add social. One of the things that keeps me up at night is how well trained are my election staff to make sure they're not clicking on links they shouldn't be clicking on? And——

Mr. TONKO. OK.

Mr. KELLEY [continuing]. That's really in the weeds, I know.

Mr. TONKO. Thank you. And, Mr. Kelley, help us understand how the paper trail works, and why it is important. When you talk about establishing a paper trail in all voting jurisdictions, what does that paper trail look like, and why does it need to be readable by humans?

Mr. KELLEY. Yes, sir. So I'll just give you a quick example. In California, we're required to have a paper trail in our electronic voting booths, and that paper trail prints out, the voter can look at that, and see what their selections were before casting their ballot. They don't take that with them, but it's included as part of the official record. The reason that's very important is because that is the official record. When you go back in a recount or an audit, you're looking at that paper record. You're not looking at the cast vote record, or the electronic portion of that ballot cast, so it has to be human readable so anybody looking at that can determine what are the true results here?

Mr. TONKO. Thank you. Thank you very much. And, with that, I yield back, Madam Chair.

Chairwoman STEVENS. Thank you. And now the Chair would like to recognize Mr. Balderson for 5 minutes of questioning.

Mr. BALDERSON. Thank you, Madam Chair. Good afternoon, everyone, thank you all for being here. Dr. Romine, my home State of Ohio is requiring all 88 counties to request a risk assessment from the Department of Homeland Security by next month. Can you speak how the suggestions NIST lays out in the Voluntary Voting System Guidelines can mitigate common mistakes found in DHS' assessments?

Dr. ROMINE. I'm not sure that I would do exactly that. What I can say is the Guidelines that we promote through the EAC are intended to guide election officials to understand what the priorities are. The DHS program of assessment is an independent activity that I think is valuable to many localities in trying to determine whether they have adequately protected and thought of all of those particular issues.

Mr. BALDERSON. OK. Thank you. My next question is for Dr. Benaloh. Dr. Benaloh, does an end-to-end verifiable system, like has been suggested by some, replace current technologies, or can it be used alongside them to ensure integrity in our election system?

Dr. BENALOH. It can absolutely be used alongside. End to end verifiability offers an independent pathway by which voters can check for themselves that the election results are correct. It doesn't need to replace current systems at all. It can be entirely separate and parallel.

Mr. BALDERSON. Thank you very much for your answer. Madam Chair, I yield back my remaining time.

Chairwoman STEVENS. Thank you to the gentleman from Ohio. And at this time the Chair would like to recognize Mr. Beyer for 5 minutes of questioning.

Mr. BEYER. Thank you, Madam Chair, very much. And thank you very much for holding this long overdue hearing. Last Congress, I repeatedly asked our former Chair to hold hearings on election security after all of the reports about Russian interference, and now, certainly, our fears have since been confirmed. They've been verified, and I'm really concerned that the Trump Administration and the Senate Majority Leader refuse to take action.

You know May 2017, President Trump announced the bipartisan Presidential Advisory Commission on Election Integrity, and appointed Kris Kobach as his Chair, despite what we now know about his concerns about his connection to white supremacy. And the formal charge of the commission was to investigate voter fraud. This is the step that Mr. Trump took after making the unsubstantiated—claim that three to five million people voted fraudulently in the 2016 election, and it appears the primary purpose of this commission was just to try to support that contention that he had somehow won the popular vote. In one of its only actions, the commission asked States to send in all their voter registration lists, including personal information like Social Security Numbers. In return, the commission mostly received just lawsuits, and then Trump decided to disband it.

Mr. Kelley, as an election administrator, and a general expert with a lot of experience, how frequently do we see actual voting fraud, where individuals actually cast fraudulent votes?

Mr. KELLEY. Well, thank you, sir. I can speak to my jurisdiction only, and in Orange County there have been very few prosecutions for voter fraud in general. I will tell you the majority of those have been under voter registration, so individuals who are out registering individuals to vote, they may change information on the voter registration cards. We have not seen any instance of in-person voter fraud, where someone would show up in a polling place and present themselves as somebody other than who they say they are. It's mainly been on the voter registration side. In the last 15 years I would say there's about five to six instances that have been prosecuted.

Mr. BEYER. Yes. In 40 years of doing politics in Virginia, I can remember exactly one instance that at least made it to the newspaper, and that was a former State Senator who had moved between his last election, voted one place, and then forgot, and voted the other place. He pled guilty, and was—can any of our panelists explain to use concisely the difference between voter fraud and election fraud? Is there—then let's move on. How about Dr. Benaloh? Given what we learned today about the information about the security and vulnerabilities in data, how much risk would there have been if the States had complied with the commission's request, and sent in all that data, including Social Security Numbers?

Dr. BENALOH. It's very hard to say. Much of the data, I believe, that was requested was public, but certainly there were non-public data that were requested. The more hands that touch sensitive data, the more exposure there is, and transporting is always a somewhat risky endeavor, but it can be done well. It should be done well.

Mr. BEYER. Mr. Kelley and Mr. Ziriax, you're both on the front lines. Do you feel you've received enough resources to be fully prepared for the 2020 election?

Mr. KELLEY. No, sir. I think we've made tremendous strides in the right direction, but I think funding is always an issue. I will say that I am grateful for the funding that we have received, because we've been able to start securing new systems in California, and that will be a leap forward for 2020. But I would never sit here and tell you, sir, that we're 100 percent.

Mr. BEYER. And Mr. Ziriax?

Mr. ZIRIAX. Thank you for the question. In the election business, we never have enough resources, no matter which particular issue you're talking about, I think. But in general I'm very grateful for the Federal funds we've received. We—just as we were with our initial HAVA funds, have been actually a little slow to spend the security funds that were granted last year. We've actually begun by spending our State match first, but—and while we do have a list of items we provided the Election Assistance Commission, we're actually reviewing those with our State Cyber Command, because there may be some additional changes that would be more cost-effective, given the limited dollars. But I would repeat what I said in my opening statement, sustained funding is better, and the

fewer the mandates, the more likely you are to get State participation in the grant process.

Mr. BEYER. Ok, great. Well, thank you very much, and thanks for being here this afternoon. Madam Chair, I yield back.

Chairwoman STEVENS. Thank you to the gentleman from Virginia. At this time the Chair would like to recognize Mr. Gonzalez for 5 minutes of questioning.

Mr. GONZALEZ. Thank you, Madam Chair, and thank you, everybody, for being here today on this incredibly important topic. To Mr. Ziriax and Mr. Kelley, you both have unbelievably important and critical jobs in securing our democracy, and I thank you for your service to your States, and by default to our country. We in Ohio have an outstanding Secretary of State, Frank LaRose, and I share Mr. Ziriax's opinion that I have no interest in dictating to him how to do his job. I trust him, I voted for him, as did many Ohioans, and I think it's our responsibility, at the Federal level, to empower you to do your job as effectively as possible. And, specifically, one area where I think we can do a better job at the Federal level is helping on a cybersecurity standpoint.

Dr. Benaloh, I want to start with a question for you. One thing we hear on the Financial Services Committee, on that Committee, and across industry, is if you don't believe you've had a cyber attack, it's because you're just not aware of it. Would you share that opinion?

Dr. BENALOH. I think that's a reasonable adage. I'm sure there are exceptions to that, but not knowing—not having seen an attack does not mean that it, in fact, did not happen. That's certainly true.

Mr. GONZALEZ. Absolutely. And then I guess my follow up, then, for Mr. Ziriax is, with that in mind, how can we better equip you, how can we better prepare you for the coming election, and going forward, from a cybersecurity standpoint?

Mr. ZIRIAX. Thank you for the question. In my opinion, continuing the Federal partnership that we have locally is something that is going to be very helpful. I know that our local FBI field office, local Department of Homeland Security officials have been very helpful, whether it's sharing intelligence, whether it's providing physical security assessments, and I think making sure that those functions are funded, and perhaps staffing is expanded. There are only two U.S. Department of Homeland Security officials, I believe, in the entire State of Oklahoma, and one of them is attached to our State Fusion Center.

But, you know, for me personally, I think making sure that funds are available, and not just funding, but the expertise and resources are available to election officials to help us secure our own systems.

Mr. GONZALEZ. Thank you. And, Mr. Kelley, same question.

Mr. KELLEY. Yes, sir. Similar answer, but I would tell you that in California we have 58 counties. Most of those counties have not taken full advantage of all of the services that DHS has to offer. I've done that in Orange County, but I think additional resources for training and pushing that—those resources out is very important, and the backlog, because it's taken a little bit of time.

Mr. GONZALEZ. Got it. And then switching to VVSG generally, and then 2.0, Dr. Romine, it strikes me that one of the hardest parts of this is we are playing an asymmetric dynamic game, es-

sentially, right? You're only as good as kind of the last set of guidelines that you've articulated, and the hackers are always kind of one step ahead. And so, with that in mind, I guess how should we think about updating your mandates, from a VVSG standpoint, to make sure that we are ahead of the game, or at least not, you know, in this world where we're doing it every couple years? It seems like we'd want to be continuously updating this information.

Dr. ROMINE. Thank you for the question. I think you've just articulated one of the reasons why the high-level principles approach to VVSG 2.0 was the way that we felt most comfortable, because at the high-level principles, they're not necessarily affected by changes in technology more than specific guidelines would do, and it gives you the opportunity to frame how you can secure the systems at a higher level.

Mr. GONZALEZ. Great. Dr. Benaloh, same question.

Dr. BENALOH. Yes. I think the high-level principles and guidelines are very valuable, and they afford the opportunity, if it is taken, to formally adopt just the high-level principles, which are far more enduring, and allow administrative revision of the detailed requirements of VVSG to be made and adjusted, as necessary, over time to accommodate changing circumstances.

Mr. GONZALEZ. Fantastic. Thank you, and I yield back.

Chairwoman SHERRILL. Thank you. Ms. Wexton for 5 minutes.

Ms. WEXTON. Thank you, Madam Chair, and thank you to all the witnesses for coming to testify today. I also want to thank the Chairwomen for holding this hearing. This is a topic that's critical to both our national security and the integrity of our democracy, so I'm very delighted that we're having this hearing.

Now, my home State of Virginia was one of the States that was targeted by Russian hackers in the 2016 election, and at the time we were using direct recording devices, or paper-free voting machines, although paper ballots were available in many polling places. And my State has now transitioned back to using paper ballots, and they expedited that transition as a result of the hacking attempt, but it seems like NIST has been sounding the alarm about insecure voting machines for a long time.

In the 2007 discussion draft paper of—to the EAC, a subcommittee of the Technical Guidelines Development Committee wrote, NIST does not know how to write testable requirements to make direct recording devices secure, and this recommendation is that the DRE, in practical terms, cannot be made secure. Is that familiar to you, Dr. Romine?

Dr. ROMINE. It is.

Ms. WEXTON. OK. And in 2011, the NIST working group on auditability concluded that voting systems that do not provide a voter-verified paper ballot will be vulnerable to undetectable hacking, and cannot be audited effectively for errors in the vote count. Is that also familiar to you?

Dr. ROMINE. It is.

Ms. WEXTON. OK. So—but it doesn't seem clear—seem to be clear that election officials at the State and local levels are getting that warning, NIST's warning, and the alarm bells that you guys are sounding about the inherent insecurity about paperless DRE (direct recording electronic) systems. Even the former Chair of the

EAC, Tom Hicks, testified to the House Homeland Security Committee earlier this year that a compromised DRE could be effectively audited to discover a manipulation. Were you aware of that testimony?

Dr. ROMINE. I believe I was on that same panel.

Ms. WEXTON. OK. Can you explain that discrepancy, or did you agree with that statement by the—by Mr. Hicks?

Dr. ROMINE. So I don't remember the context in which he made that statement. I think possibly what he was alluding to was a collection of recommendations for auditability that might include risk-limiting audits. So there are certainly opportunities for advanced statistical analysis to be able to reveal the potential presence of anomalies in voting, but I don't remember exactly whether he was endorsing fully paperless ballots or not.

Ms. WEXTON. So going forward, how can we ensure that NIST's research and conclusions regarding the security and auditability of DREs are given due attention and shared effectively with election administrators to inform policy?

Dr. ROMINE. We have strong relationships with the National Association of State Election Directors, NASED, and other venues for State officials, and we talk regularly with them. Many of the stakeholders participate in the working groups, the cybersecurity working groups, a working group that I alluded to earlier, with 175 members. So we're getting the word out. There's some awareness building. The principle guideline, from our perspective, is the necessity of an audit mechanism. Our Guidelines don't specify how that audit mechanism is to be done, but the importance of auditability is essential, and our guidelines reflect that.

Ms. WEXTON. Very good. Thank you. I will yield back with that.

Chairwoman SHERRILL. Thank you. Dr. Marshall? He's gone? OK. And so we are now down to Mr. Waltz for 5 minutes.

Mr. WALTZ. Thank you, Madam Chairwoman, and I want to thank everyone for holding this important hearing. I have some concern on the timing of it. I think this hearing is absolutely necessary, and would have hoped we could work toward some bipartisan solutions before the majority put the bill H.R. 2722 forward this week, that is looking to put $1.3 billion at this issue.

Here nor there, I am working with Representative Stephanie Murphy and putting together an alerts framework. We all know I represent Florida, and we all know that two of Florida's counties were breached as a result of a Russian spear phishing campaign targeted at county election officials. None of the congressional delegation, nor the State officials, were notified by the FBI or DHS as a result of that intrusion in 2016. The bill that we are working would seek to correct that problem. Not only should officials be notified, but Floridians, and the voters, should be notified, in the guise of maintaining confidence in our electoral system.

So part of the issue was that the Russians targeted employees of a Florida-based manufacturer of voter registration software, VR Systems. VR Systems has confirmed to the media that they were the company that was penetrated. They have responded to a letter from Senator Wyden that they did not click on an attachment in the e-mail, however, we do know that VR systems used remote access software on election management systems it sold to the coun-

ties leading up to that 2016 election. We don't know if the systems were hacked as a result of the remote access software, and DHS is conducting forensic analysis, I promise you I'm getting to my questions.

Look, at the end of the day, the company responded that they had been following the NIST cybersecurity framework that we've talked about prior to 2016, and they continue to do so today, so this gets to my question, Dr. Romine. Under HAVA, NIST is directed to develop the VVSG, all right, we know that. The law defines voting systems for the purposes of mandating NIST to create standards for testing and certifying voting systems. Not included in the definition of voting systems, which I know we've gotten to somewhat today, but I want to really spend time on this point, not including the definition of voting systems are voter registration panels and voter registration databases. And, because of this, there have been questions whether this vendor in particular, but I think it's a broader question, whether this vendor, VR Systems, implemented NIST framework, because, again, there's issues now with the definition.

So although NIST guidelines are voluntary, and you're not a regulatory agency, which I think is correct, regardless of whether the standards meet the definition of voting systems under law. So question one, how would authorizing voter registration portals and databases under the *Help America Vote Act*, under HAVA, improve NIST's ability to provide innovative standards with respect to registration technologies?

Dr. ROMINE. Thank you, Mr. Congressman. The guidelines that we currently provide under HAVA, the scope of those guidelines is controlled largely by the EAC, who makes the determination of what is in scope, or it's their interpretation of HAVA. The role that we play in cybersecurity broadly allows us the opportunity to provide things like the cybersecurity framework and other guidance on more traditional IT type systems, such as those that generally are used for voter registration databases, and e-poll books, and so on. So we already have guidelines in place that might be applicable. The change there would be that those guidelines would be incorporated into the EAC database, for example, for VVSG guidelines, and that would be perceived as more directly relevant to election officials.

Mr. WALTZ. I am out of time, but could you submit for the record how doing so, and how changing those guidelines, would incentivize companies and vendors, for example VR Systems, and other registration software companies to follow NIST guidelines, and implement the framework?

Dr. ROMINE. I'll be happy to respond.

Mr. WALTZ. Thank you. I yield my time.

Chairwoman SHERRILL. Thank you. And next the Chair recognizes Ms. Horn for 5 minutes.

Ms. HORN. Thank you, Madam Chair, and thank you for allowing me to join this Subcommittee on such an important issue today. I—we have covered a lot of ground today, and in—this is such a critical topic. I want to tackle a couple of questions for I think most of the panel, just in a slightly different direction. It seems to me—I've heard both Dr. Romine and Mr. Ziriax say very clearly and ex-

plicitly that we have to work to balance being—the accessibility and convenience, and making sure that people can show up and cast a ballot, and not making it so hard to cast a ballot that we disincentivize participation in the system, with a reliable and secure system. I absolutely agree, and this is a challenge to balance.

And, Dr. Sweeney, in your presentation, in your testimony, we're looking at two sides of this coin. We're looking at the voting system, and the ability to verify votes, and the security, but also the database, and so we've got two different pieces to this, as I see it. So I want to start with the verify—the piece of—the verification, and how we can put parameters around that to continue to ensure the confidence and the auditability of our voting systems.

I noted, Mr. Ziriax, in your testimony, in your presentation, that Oklahoma, and I think Chairwoman Stevens mentioned this as well, has three, as I see them, fundamental baseline principles that help the ability to verify and audit votes, paper ballots, a Statewide system that is uniform, and owned by the State, which helps allay differences between the different counties, and the fact that the systems in Oklahoma aren't connected to an Internet source, which is another challenge. So my question—and we've talked about how we set these standards, the VVSG 2.0, VVSG, that—it seems that we have States that aren't even getting up to the baseline. So I—Mr. Kelley and Mr. Ziriax, I'd like to hear your opinions about the need to set baseline standards that all States have to comply with, of course assuming we're going to help provide the funding at the Federal level to help with that.

Mr. ZIRIAX. Thank you, Ms. Horn, and I think there's, you know, there's a fine line between, say providing the guidelines, and allowing the States to determine how best to do that. And some things—I mean, just to give an example, and, again, these are similar things that I've discussed with—about other election bills, but the bill that's been discussed earlier today, the *SAFE Act* (Securing America's Federal Elections), includes a mandate that new voting systems have to accommodate ranked choice voting, for example, and that's in an election security bill.

Me personally, you know, I view that as a decision that our State should make, whether we want to move toward that. But if Congress is going to provide money, and wants to say, if you want our grants, then you need to at least demonstrate that you're going to attempt to follow the voluntary guidelines, that's certainly Congress' prerogative.

Mr. KELLEY. And I would concur with that. I would just also add that—for the—for an example in California, there is an enhanced requirement in California for certification, so it just does not rely on the Federal standards, it goes above and beyond that. And I think I would agree also that the States should, in many cases, make those decisions, personal opinion.

Ms. HORN. Thank you. Now turning to the next piece of this is—that we—we're going to have to face, Dr. Sweeney, you referenced all of the ways that individuals could perhaps get into different systems without necessarily verifying their identity. So, knowing that there are a range of challenges that we may not even know, and, Dr. Romine, you've spoken to some of these as well, do you see any other pathways, or potential solutions, for example bio-

metrics, or anything like that, that would help, moving forward, to protect these systems?

Dr. SWEENEY. I think the most immediate answer is probably just to follow the best practices of things like using driver's license, but it is a—with additional information off the driver's license, and using a modern capture device. But it is a bit of a moving target, because that's not wholly satisfactory. That—it requires a bigger question about how we authenticate. The problem, though, is it's—the questions that you pose generally around what NIST has proposed and so forth, and it was brought up that a lot of what they talked about happened years before they started saying it. I'm like that, but now years before.

And, you know, so there's a—so we have a cycle mismatch as well. So I think, if we're going to do the cycle, if we could move faster to, like, implement something like, OK, what's the best practice right now, to nail that down, like the driver's license, then we have a better shot at not being victimized by it, and having to come back in a few years, and say, well, how many States have improved what they asked for?

Ms. HORN. Thank you very much. So we both have to address the challenges now, and look forward—thank you all for your testimony. I yield back, Madam Chair.

Chairwoman SHERRILL. Thank you. And now I would like to recognize Mr. Sherman for 5 minutes.

Mr. SHERMAN. I want to agree with Mr. Ziriax that the Federal Government has no business pushing rank choice voting, or rank order voting. Those who propose it most are those who most want to undermine the two party system. There are arguments for and against having two major parties in this country, but that's not something that the Federal Government should be pushing on the States.

My first question is for whichever panelist answers it first. What number of States currently require the use of paper ballots and an auditable paper ballot trail? Do we know how many States do that? I thought there'd be a jump in to be the first to answer.

Mr. ZIRIAX. Oklahoma does.

Mr. SHERMAN. And I guess the other States don't matter. Do we have—if we don't have that, then I'll ask whichever witness raises their hand first to agree to answer that for the record.

Dr. SWEENEY. I——

Mr. SHERMAN. Do we have any hard working——

Dr. SHERRILL. I do believe——

Mr. SHERMAN [continuing]. Witnesses?

Dr. SHERRILL [continuing]. Five do not. I know——

Mr. SHERMAN. Five do not?

Dr. SHERRILL [continuing]. I know New Jersey does not.

Mr. SHERMAN. Got you. Hopefully it's only five that do not. For States which conduct testing and certification of voting machines, how do the State standards compare with the standards promulgated by the U.S. Election Assistance Commission? Yes?

Mr. ZIRIAX. I can—as Oklahoma's chief election official, I can only talk about our State. I know with our current system, which was implemented in 2012, although our State law does not require that we follow those guidelines, the guidelines that I set at the

time, when we were reviewing that system, and requiring testing for it, we did require testing to ensure compliance with many of the VVSG 1.0 requirements.

Mr. SHERMAN. Anyone else have a comment?

Mr. KELLEY. Yes, sir, just very quickly, in California it's very similar, VVSG 1.1, but I will say one of the key differences is that California requires volume testing of all the systems, where those are not in the current standards.

Mr. SHERMAN. Should they be added to the national standards?

Mr. KELLEY. Sir, if I could defer that question?

Mr. SHERMAN. OK. Increasingly a number of States, including my own, has moved to vote by mail. My State has authorized ballot harvesting. I'm told that the proponents of it would prefer I call it by a different name. What technologies do we need to prevent either false registrations, followed by false vote by mail voting, where—knowing that people who—people are not looking to cheat by adding one vote. I know every vote matters, and we—but those who want to steal votes want to do it by the—at least by the hundreds. What do we do, first, to prevent false registrations, followed by false voting, all done by mail? Is there any system that is designed to combat that?

Dr. SWEENEY. I wouldn't say that it's—I'm not answering exactly on——

Mr. SHERMAN. Right.

Dr. SWEENEY [continuing]. Point to you. It's not so much that it's designed to combat it, it's just that it's totally a different vector than has been really talked about in computer security, because I'd use the change of address, but it—what we also talk about, it could be absentee ballots. I—disenfranchise a person who then would go to the voting place, who would get a provisional ballot, and that ballot won't count, or in the case of a State where it's vote by mail.

Mr. SHERMAN. If I can squeeze in one question? In my State they compare the signature on the outside of the envelope to the signature on the voter registration card.

Dr. SWEENEY. Right, but the clarification here is not——

Mr. SHERMAN. I've got to squeeze in one more question, I'm sorry. Mr. Kelley, or anyone else, is that process useful at all? Do the people who do that have any expertise in comparing signatures, and do signatures change over time? My voter registration form was filled out long, long ago.

Mr. KELLEY. Yes, sir. I'm glad you asked the question, because absolutely they do, and you see that, especially with historical signatures that we have on file. 20 years, 30 years, you see a big difference. I will add that——

Mr. SHERMAN. So what percentage of the ballots in our State is—are put aside or provisional because there's some question as to whether the signature is legitimate?

Mr. KELLEY. One plus million ballots cast in Orange County by mail, we had about 5,000 that were set aside specifically for signature issues. Now, I will——

Mr. SHERMAN. How many of those were ultimately counted, how many of those were not ultimately——

Mr. KELLEY. The majority were ultimately counted. California changed its law last year to allow us to reach out to the voter to attempt to cure that.

Mr. SHERMAN. And so you had to reach out in 5,000 circumstances and say, hey, is this really your signature.

Mr. KELLEY. Yes, sir, we did.

Mr. SHERMAN. Wow. I believe my time has expired.

Chairwoman SHERRILL. Well, thank you, and now the Chair recognizes Mr. Casten for 5 minutes.

Mr. CASTEN. Thank you, Chairwoman Sherrill. Thank you to the panel. The—one of my favorite things about this Committee is we consistently get such fascinating nerds before us, and you guys are all awesome. Just—learned so much today on a really important topic. And fortunately, the nerds are not just limited to the panel. The—I want to thank—there's a few of us up here, but I want to thank our young visitor, Bianca Lewis, for being here. Really, really appreciate what you've done.

And I want to talk a little bit about, if I understand what you did at DEFCON—my understanding, if I've got it right, is the method that the participants in your exhibit used to hack into the Secretary of State website was called a sequel injection? And—I got it right? The—this is—the single strategy that these kids at DEFCON demonstrated is also what is described in Robert Mueller's report that the Russians did.

Page 50, Volume 1, of the report says the following, GRU officers—Bianca, GRU is the Russian agents—targeted State and local databases of registered voters using a technique known as sequel injection, by which malicious code was sent to the State or local website in order to run commands, such as exfiltrating the database contents. In one instance, the GRU compromised the computer network of the Illinois State Board of Elections, my State, by exploiting a vulnerability in the State Board of Elections website. The GRU then gained access to a database containing information on millions of registered Illinois voters, and extracted data relating to thousands of U.S. voters before the malicious activity was identified. This is real-time stuff. But what it seems to be saying is that the Russians used a real sequel injection to crack open the real State website, same strategy that Bianca demonstrated on the models at DEFCON, and then the Russian worm kept going all the way through to the voter registration database.

Now, Illinois has done great work in responding to this. I hope we have done enough. We seemed to be OK in the last election, but this is really scary stuff. And—so what I'm—first I'd like to ask unanimous consent to add pages 50 and 51 of Volume 1 of the Mueller Report, which describes this episode, to the hearing record.

Chairwoman SHERRILL. Without objection.

Mr. CASTEN. And then, notwithstanding how I started this, I want to start with Dr. Benaloh. Could you explain to us, so that us smaller-brained people up here can understand, how does a sequel injection work, exactly?

Dr. BENALOH. You're getting a little bit away from my expertise, but the basic idea is that the—in a web query of some—of any sort, additional information can be added to what's—what would otherwise be interpreted as an innocuous web request that is not of the

form that's expected by the web server that is handling this request. And if there aren't adequate measures in place, that web server may interpret that additional information as code to be executed, and to potentially do harm, or provide services that are not intended by the——

Mr. CASTEN. Essentially modifying an existing sequel SQL database?

Dr. BENALOH. Yes. It——

Mr. CASTEN. Dr. Sweeney, I see you nodding your head. Is there anything you want to add to that? Did I get it about right?

Dr. SWEENEY. No. I mean, that's about right. The idea is I just simply can add commands within a command so that it'll, in fact, do multiple things that never—you never intended me to do. You provided access, say, to list some voters, or to check one voter, and I just end up deleting 1,000, or downloading a million, or something like that.

Mr. CASTEN. So, for all of you, is this an—is this a technique we should expect to be seeing again, and be watching for? I see a lot of head nodding will be entered into the record. Dr. Romine, does NIST's work in VVSG address the need to firewall State websites, particularly under the voter registration databases, that we can protect against this in some fashion?

Dr. ROMINE. I actually don't know the answer to that, but I'm happy to respond to that. I suspect that it does, but I can't confirm that. I'll have to go back and check.

Mr. CASTEN. That would be very helpful to find out.

Dr. ROMINE. Happy to do that.

Mr. CASTEN. Thank you all, and I yield back the balance of my time.

Chairwoman SHERRILL. Thank you, and now the Chair recognizes Mr. McAdams for 5 minutes.

Mr. MCADAMS. Thank you, Madam Chair. I think this timely hearing is important for our Congress to review the current efforts, and the plan—and to plan our future work to develop—or to protect our elections from malign actors. So this work will require, I think, strong collaboration from local, State, and Federal partners to ensure the integrity of our elections, and that all Americans can participate in our democracy. In my previous role, I was one of those local officials. And, while I wasn't a county clerk, per se, was familiar with the incredible work that they do to protect the integrity and security of our elections, and sometimes under very difficult circumstances, but I applaud, and am grateful for those elected officials across the country who work with the greatest effort to protect our elections.

And I'm also proud that my home State of Utah has been leading the way in upgrading our election infrastructure and policies, and also cybersecurity practices. Our county clerks, in 2018, led the substantial upgrade—a substantial effort to upgrade voting machines, and also to take other security measures in advance of the 2018 midterms, while also promoting more options for Utahans to vote, including adopting things like widespread vote by mail, and same day registration. Utah is one of 17 States that offer same day registration, and I believe policymakers should support any strategy that makes it easier for Americans to add their voice to our de-

mocracy, so long as our election practices maintain the high standards of security and integrity.

So I'd like to discuss the implications for same day automatic, or any mode of registration on our election system security. So to anyone on the panel who'd like to respond, how can same day registration help to mitigate the effects of a cyber attack on voter registration data close to the election? Are there any concerns we should be worried about with that?

Dr. SWEENEY. I would say the same day registration could definitely be a way of resolving the threat that I described. And the reason being that if somebody—if a malicious actor had come in and intended to disenfranchise a large percentage of those voters, but those voters still show up at their polling place, and could register right there, the attack would be thwarted.

Mr. MCADAMS. Yes.

Mr. ZIRIAX. And if I may add, in Oklahoma, my State, we do not have same day voter registration, we have a 24-day deadline. I don't anticipate anywhere in the near future that that is going to happen, but we extensively use the provisional ballot process in Oklahoma, so then, in the event you did have a situation where perhaps large numbers of voters were not appearing on registries, we would have a backup means, and then be able to go back and confirm later that those people actually were eligible to vote.

Mr. KELLEY. Similar comments in—from California, and I would say that the same day registration growth in California is growing, but it is small. It's still a small number compared to the overall database. So I think we need to be careful and just say that's the solution. We should be looking at the database as a whole, and finding ways to detect anomalies in that database itself.

Mr. MCADAMS. So I guess my second question relates to automatic voter registration, and how can that operate in a secure election system. And ultimately is—are election security and automatic voter registration, are they in competition, or they—are they in symbiosis?

Mr. KELLEY. I don't think they're in competition. It's certainly a different dynamic when you go into DMV, for instance, in California, and it's automated registration that you could opt out of, where same day registration is you're affirmatively going to a polling place, or vote center, to register to vote. So I don't think they're in competition with each other.

Dr. SWEENEY. From a security standpoint, it definitely would change—if I wanted to disenfranchise voters, because—in those States, where provisional ballots don't fully count, then I would just want to attack the database. So it would remove the—automated registration might remove on one layer—but remember the attack that I talked about was changing an existing——

Mr. MCADAMS. Um-hum.

Dr. SWEENEY [continuing]. Registration, so it would still allow that.

Mr. ZIRIAX. And if I may, I want to briefly add that, you know, some of the concerns Dr. Sweeney and others have expressed about the vulnerabilities for online voter registration, if you're talking about whether you have the ability to confirm a person's identity,

or whether someone could use a stolen identity to register to vote falsely, that could happen with paper ballots now.

Dr. SWEENEY. Let me make just one quick correction, since I was called. I——

Mr. MCADAMS. Yes.

Dr. SWEENEY [continuing]. These are not voter registration systems. I'm not talking about voter—it just happens that sometimes changing the voter record is on the same system as the voter registration website, but sometimes it's on the DMV site. I'm only talking about registrations that already exist.

Mr. MCADAMS. And these are policies that would protect our elections. So I see our time has expired, and, Madam Chair, I yield back.

Chairwoman SHERRILL. Well, thank you very much. And thank you so much to all of the panelists today. I think all of us think this is such a critical issue moving forward. Thank you to Bianca. You are not only a STEAM wizard, you are a trooper to sit through our hearing today, so I appreciate everyone here today. Thank you very much, and hopefully we will be talking again. Maybe we can get you in, Dr. Romine, for your 21st appearance. So thank you all very much. Thank you.

[Whereupon, at 4:58 p.m., the Subcommittees were adjourned.]

Appendix I

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Dr. Charles H. Romine

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON INVESTIGATIONS & OVERSIGHT
SUBCOMMITTEE ON RESEARCH & TECHNOLOGY

Election Security: Voting Technology Vulnerabilities

Questions for the Record to: Dr. Charles H. Romine
Director, Information Technology Laboratory
National Institute of Standards and Technology

Submitted by: Representative Michael Waltz (FL)

1. It is my understanding that voter registration systems (including online portals and backend databases) fall outside the scope of a "voting system" as that term is defined in the Help America Vote Act (HAVA). How might expanding HAVA to encompass voter registration systems help incentivize companies that produce voter registration software and systems to build to the criteria established in the Voluntary Voting System Guidelines? Additionally, how might the Election Profile for the Cybersecurity Framework help to accomplish the same?

   NIST Response: The definition of a "voting system" in the Help America Vote Act does not address voter registration software and systems. Voting system security requirements (including access control, data protection, system integrity, and logging) developed under the Voluntary Voting System Guidelines (VVSG) 2.0 for voting systems also apply to voter registration software and systems. However, online voter registration systems connected to the Internet increase the threat surface beyond those of voting systems. Within the current statute, testing and certification is limited to voting systems; thus, testing and certification of voter registration systems is not authorized. Expanding HAVA to encompass voter registration systems would permit the development of guidelines, and a testing and certification program that would ensure voter registration systems are free from known vulnerabilities. A combination of cyber-hygiene and software patching could help to detect and mitigate against new vulnerabilities after systems are deployed.

   The Election Profile for the Cybersecurity Framework would take a holistic approach to securing voter registration systems by providing concrete steps that election officials, vendors, and their information technology staff can use to improve their cybersecurity posture. It considers not only the software and systems, but also risk assessment, communications, governance, cyber-training and cyber-responsibilities, and ongoing monitoring, detection, and mitigation. In a sense, it serves as a cyber playbook for the intended systems. The profile maps specific security controls to high-level mission objectives, enabling communication among election officials and the information technology staff. Specific security controls can apply to both the voter registration software and systems and the networks on which they run. Verifying that the controls are properly implemented within the software and systems will still require a testing and certification program.

Asked by: Representative Casten (IL)

2. Does NIST's work in VVSG address the need to firewall state websites, particularly under the voter registration databases, that we can protect against this in some fashion?

   NIST Response: The scope of the VVSG is limited to the voting systems themselves and does not include additional election systems, such as the voter registration databases. The voting systems are those that activate, mark, and count the ballots.

Responses by Mr. Neal Kelley

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON INVESTIGATIONS & OVERSIGHT
SUBCOMMITTEE ON RESEARCH & TECHNOLOGY

Election Security: Voting Technology Vulnerabilities

Questions for the Record to:
Mr. Neal Kelley
Registrar of Voters
Orange County, California
Submitted by: Representative Suzanne Bonamici (OR)

- Mr. Kelley, the National Academies Securing the Vote report makes clear that Risk-Limiting Audits are the gold-standard for establishing resilient and secure elections. The Oregon legislature recently passed Senate Bill 944, an election security bill that will extend state requirements for post-election audits to include special elections in addition to primaries and would also allow risk-limiting audits (RLAs) as an alternative to hand recounts. I'm curious how these audits operate on the ground. Most of the examples the Committee has observed in the press and in background materials describe audits being done on central-count scanners. Orange County conducted an RLA pilot last year. Can you tell us what kind of voting equipment you have in Orange County, whether RLAs be conducted on all election technology, and walk us through what, if anything, was unique about your process?

Response to Representative Bonamici's Questions for the Record

In 2018, the Orange County Registrar of Voters concurrently conducted the 1% manual tally and a risk- limiting audit pilot program to compare the use of statistically based audit techniques and traditional post-election audits. To serve as an example to jurisdictions that may consider conducting a risk-limiting audit, Orange County successfully conducted two risk-limiting audit pilots using its legacy voting system. The first pilot was conducted in two phases during the June 2018 Statewide Primary Election and the second pilot was conducted during the November 2018 Statewide General Election.

While we are transitioning to a new voting system, the system in use during the 2018 Pilot RLAs was the Hart Intercivic, HVS v. 6.1, which is known as a legacy system (originally certified under the 2005 VVSG standards).

What was unique about this process is the lack of a cast vote record to conduct a comparison audit - this meant that we had to conduct a ballot polling audit (another form of RLA), which matched the physical ballot with the originally tallied results. This is still a very effective form of audit for legacy systems, but it is not as precise as the comparison audit.

I do believe that these types of audits should not be limited to the ballots themselves, for instance conducting audits on the ballot creation process is an important form of audit, among others.

What was also unique were the logistics of organizing nearly 2 million paper ballots in order to find the needles in the haystack - this is (I believe) one of the most daunting aspects of conducting ballot polling audits for election officials - they simply do not have the tools, resources and background in most cases.

I have attached a report that details the pilots that we conducted, which should shed additional light on our RLA pilot process.

Thank you,

Neal Kelley
Registrar of Voters
Orange County, CA

Responses by Dr. Josh Benaloh

Microsoft Innovation & Policy Center
901 K Street, NW 11th Floor
Washington, DC 20001

Tel 202-263-5900
Fax 202-783-0583
http://www.microsoft.com/

Microsoft

July 23, 2019

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON INVESTIGATIONS & OVERSIGHT
SUBCOMMITTEE ON RESEARCH & TECHNOLOGY

Election Security: Voting Technology Vulnerabilities

Questions for the Record to:
Dr. Josh Benaloh
Senior Cryptographer
Microsoft Research
Submitted by: Representative Suzanne Bonamici (OR)

- Dr. Benaloh, Microsoft worked with several partners, including Portland-based Free and Fair, to develop "Election Guard." How can this new tool help with auditing paper-based systems and why is it important that the software be open-source?

  Dr. Josh Benaloh: ElectionGuard enables two types of audits. One is a public audit using the mechanism of "end-to-end verifiability". This allows voters to directly check for themselves that their votes have been correctly counted – without having to trust anyone at all, and with full privacy and protection from coercion. End-to-end verifiability can democratize the electoral process by shifting power from those who control the counting of votes to the voters themselves.

  The second type of audit enabled by ElectionGuard is an improved form of more traditional administrative audits (including risk-limiting audits). ElectionGuard enhances the privacy of voters in so-called "ballot-comparison audits" – the most efficient variety of administrative audits. Observers can confirm the accuracy of a ballot-comparison audit without necessitating the release of the contents of all the ballots cast in an election.

  While neither the end-to-end verifiability nor the enhanced privacy provided for traditional audits requires any trust in the ElectionGuard software, public confidence is nevertheless amplified using open-source software.

Microsoft Innovation & Policy Center
901 K Street, NW 11th Floor
Washington, DC 20001

Tel 202-263-5900
Fax 202-783-0583
http://www.microsoft.com/

Microsoft

Questions for the Record to:
Dr. Josh Benaloh
Senior Cryptographer
Microsoft Research
Submitted by: Representative Bill Foster (IL)

- I understand that West Virginia and Denver, Colorado are introducing blockchain internet voting, with claims that blockchain resolves the security concerns of online voting. CNET said, "In principle, blockchain technology sounds like a great solution to today's voting system problems. It offers a way to resist data tampering, creates a foundation to enable voting by phone and can generate an instant audit to verify election results." But went on to highlight the concerns experts have raised including by the National Academies which stated, "While the notion of using a blockchain as an immutable ballot box may seem promising, blockchain technology does little to solve the fundamental security issues of elections, and indeed, blockchains introduce additional security vulnerabilities," the report said. "In particular, if malware on a voter's device alters a vote before it ever reaches a blockchain, the immutability of the blockchain fails to provide the desired integrity, and the voter may never know of the alteration."

  Can you please explain why the National Academies study did not support blockchain as a way to provide secure, reliable and auditable internet voting? What is the worst-case scenario in the districts that have already adopted this technology for voting?

  Dr. Josh Benaloh: Blockchains are an interesting new technology with some valuable applications, but they are ineffective in elections. Blockchains provide a mechanism for a decentralized set of participants to achieve effective agreement without having to rely on a central authority. This is not the environment in which elections are held.
  A public election requires a central authority to determine voter eligibility, to set the contents of the ballot, to fix the times during which voting is allowed, and to perform many other important tasks. This central authority needn't be trusted. All these actions are public, and they can be challenged if they are not performed correctly. But there needs to be a central authority who is responsible for taking these actions. Once this central authority is in place, any data that might be posted on a blockchain could instead be more easily and reliably published directly by the central authority.

Microsoft Innovation & Policy Center
901 K Street, NW 11th Floor
Washington, DC 20001

Tel 202-263-5900
Fax 202-783-0583
http://www.microsoft.com/

Microsoft

The use of blockchains also introduce new vulnerabilities to elections. For instance, Bitcoin and most cryptocurrencies use "unpermissioned" blockchains in which no entities have any special powers or privileges, and anyone can perform the duties of these entities. These unpermissioned blockchains feature a lack of direct accountability. Participants are, for instance, allowed to favor some voters over others and make it more likely that the votes of favored voters will be counted. In contrast, permissioned blockchains, offer greater accountability. But those invested with power can use that power to alter the results of an election. It can be difficult if not impossible for those without permissions to effectively monitor and police the actions of the permissioned. In neither case do blockchains address the true challenges of voting: establishing authorization to vote while providing anonymity or confidentiality together with verifiability. Cryptographic protocols can be incorporated to achieve these properties. But once these protocols are used, the blockchains themselves become entirely superfluous.

Blockchains are only meaningful in the context of online voting. A 2015 study by the U.S. Vote Foundation explored online voting in great depth and found end-to-end verifiability (using sophisticated cryptography) to be the only potentially viable approach to responsible online voting. It found, however, some fundamental problems that need to be addressed before this could be done responsibly. Probably the greatest concern is client malware on the devices of voters, and when malware can change votes before they ever touch a blockchain, the use of blockchains offers little benefit.

Put concisely, blockchains don't address any of the real challenges of today's voting systems – much less the problems that prevent us from enabling responsible online voting. Yet their use introduces significant new weaknesses and vulnerabilities to voting systems.

Microsoft Innovation & Policy Center
901 K Street, NW 11th Floor
Washington, DC 20001

Tel 202-263-5900
Fax 202-783-0583
http://www.microsoft.com/

Microsoft

Questions for the Record to:
Dr. Josh Benaloh
Senior Cryptographer
Microsoft Research
Submitted by: Representative Dan Lipinski (IL)

- Dr. Benaloh, what are some of the most pressing basic research questions in computer science and in the social sciences that are relevant to election systems security that an agency like the National Science Foundation might support?

  Dr. Josh Benaloh: Election security benefits from security advances in computer system software and hardware; so, any research directed at general computer security can be beneficial to election security. Beyond these broad strokes, there are many specific areas of focus that could provide additional value.

  Even with improved security, there is little prospect for making our election infrastructure impervious to attack. Therefore, we must devote resources to detection of and recovery from attacks. There has been significant research into verifiable election technologies that enable detection of alterations in an election record, and while this technology is on the verge of deployment, numerous challenges remain. As systems that achieve so-called "end-to-end verifiability" are deployed, we must study how well they are understood and accepted by voters and what improvements can be developed to make these systems more effective. As one example, today's end-to-end verifiable systems generally require the possibility of interaction between voters and voting devices, so while they can be used in many in-person voting scenarios, they become cumbersome when used with vote-by-mail or in environments where ballots are processed centrally rather than at poll sites. Another example is the limitations on voting rules than can be achieved by today's verifiable systems: while it is possible to accommodate most simple counting rules, more complex rules like those used in various ranked-choice voting systems create significant challenges. There is also a need to pursue systems that offer better forms of evidence that can be used by voters to convince others of malfeasance. Since these end-to-end verifiable election systems involve new kinds of interactions with voters, research on usability of these systems is also of great value.

  Other forms of post-election auditing are also in need of greater attention. While new forms of administrative audits offering better statistical properties have been developed and piloted, it is not yet understood how to best implement these advancements in elections with multiple overlapping jurisdictions. This is true in even the simplest cases where, for instance, a state-wide contest may appear on ballots from different local jurisdictions which include local contests as well. More research into this topic has the

Microsoft Innovation & Policy Center
901 K Street, NW 11th Floor
Washington, DC 20001

Tel 202-263-5900
Fax 202-783-0583
http://www.microsoft.com/

Microsoft

potential to make many post-election audits, including risk-limiting audits, far more practical and efficient.

Another area of great interest is how voting system design impacts voter participation. There is, for instance, a broad belief that the availability of online (Internet) voting would substantially increase voter participation. However, limited experience seems, surprisingly, to show that this is not the case and that use of online voting might even slightly depress participation. This and related questions concerning voter participation would be extremely valuable to understand better – as answers to these questions could influence our decisions on what kinds of election systems to build and utilize.

Appendix II

Additional Material for the Record

DOCUMENTS SUBMITTED BY REP. MIKIE SHERRILL

BRENNAN CENTER FOR JUSTICE

House Committee on Science, Space and Technology
Subcommittee on Investigations & Oversight
Subcommittee on Research & Technology
United States House of Representatives

Statement for the Record
Brennan Center for Justice at NYU School of Law

"Election Security: Voting Technology Vulnerabilities"

June 24, 2019

The Brennan Center thanks the House Committee on Science, Space and Technology for holding this hearing.

Our country has made significant progress to secure our elections infrastructure from cyber-attack since 2016. The designation by the Department of Homeland Security ("DHS") of election infrastructure as critical infrastructure means state and local election offices have priority access to needed resources, including cybersecurity advisors and risk assessments. As a result, election officials have participated in thousands of hours of cybersecurity trainings and table-top exercises to prevent, detect, and recover from intrusions into critical election infrastructure.[1] DHS and the Election Assistance Commission ("EAC") have facilitated much better information sharing between election system vendors, the states, and the federal government. Finally, in 2018 Congress provided $380 million in Help America Vote Act ("HAVA") funds to help states bolster their election security. Finally, in 2018 Congress provided $380 million in Help America Vote Act ("HAVA") funds to help states bolster their election security. Based on information provided by the EAC, we know that roughly 90% of this money will be spent prior to the presidential election on such critical measures as strengthening election cybersecurity, purchasing new voting equipment, and improving post-

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

election audits, all essential steps in protecting our elections from foreign interference.[2]

Nevertheless, significant security gaps remain. We should be doing more to secure our election infrastructure in the following areas, several of which are particularly relevant to the jurisdiction of the House Committee on Science, Space and Technology: (1) replacing paperless voting systems and requiring robust post-election audits; (2) adding electronic poll books to the federal certification process; (3) conducting penetration testing and nationwide threat assessments of the nation's election infrastructure; (4) requiring election system vendors to report cyber incidents; (5) requiring the National Institute of Standards and Technology ("NIST") to create an Election Profile to guide adoption of the Cybersecurity Framework nationwide for elections infrastructure; and (6) providing additional funding to state and local election officials to secure election systems nationwide.

Replace Paperless Voting Systems and Robust Post-Election Audits

The Brennan Center has long supported both a complete, nationwide transition to paper ballot voting machines and the implementation of risk limiting audits ("RLAs") to ensure security and confidence in electoral results.

In the event a virus or other malicious software is introduced into a voting machine, voter-marked paper ballots can be used to detect and recover from that attack. The National Academy of Sciences, Engineering, and Medicine is just one of the latest authorities to examine paperless voting systems and conclude that they should be "removed from service as soon as possible" to ensure the security and integrity of American elections.[3] They have been joined in this conclusion by the U.S. Senate Select Committee on Intelligence, as well as security experts around the country, all of whom have argued that continued use of these systems presents an

[2] *Discussion on Recommendations from the ODIHR Observation of the 2018 Mid-Term Congressional Elections,* OSCE Office for Democratic Institutions and Human Rights (June 18, 2019) (statement of Benjamin Hovland, EAC Commissioner); *Grant Expenditure Report, Fiscal Year 2018,* The U.S. Election Assistance Commission, April 4, 2019, https://www.eac.gov/assets/1/6/FY2018HAVAGrantsExpenditureReport.pdf.

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

unnecessary security risk.[4]

Today, 11 states still use paperless electronic machines as the primary polling place equipment in at least some counties and towns (Georgia, Indiana, Kansas, Kentucky, Louisiana, Mississippi, New Jersey, Pennsylvania, South Carolina, Tennessee and Texas). Three (Georgia, Louisiana, and South Carolina) continue to use such systems statewide.[5] There is still time for these jurisdictions to transition to paper-based voting systems before the 2020 presidential election. Approximately $300 million is still needed to replace the remaining paperless voting systems in use throughout the country.[6] Congress should act to ensure that every vote in 2020 is supported by a secure and verifiable record of voters' decisions, in the form of a paper back up, to help guard against electronic manipulation.

Of course, without robust election audits comparing paper records to software totals, the value of that paper record is more theoretical than actual. For this reason, we support robust post-election audits that will

---

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

[5] "The Verifier — Polling Place Equipment — November 2018," Verified Voting, accessed June 24, 2019, https://www.verifiedvoting.org/verifier/; Delaware rolled out new machines with paper backups on May 14 of this year. See Amy Cherry, "Delawareans to get 1st look at new voting machines in upcoming school board elections," WDEL, May 6, 2019, https://www.wdel.com/news/video-delawareans-to-get-st-look-at-new-votingmachines/article_7d625346-6ddd-11e9-a2c7-4f6dfafa74af.html.

[6] Relying mainly on Verified Voting data from November 2018, we estimated that approximately 37,232 precincts
are using paperless DREs as the primary polling place equipment (this number excludes precincts in Delaware which replaced machines in May 2019). We multiplied this number of precincts by $8,000, our estimate for per-precinct machine replacement cost, to arrive to our $300 million estimate.

provide voters with confidence they can trust the electronic totals provided on election night. Unfortunately, only 22 states that have paper records of every vote require post-election audits of those votes before certifying their elections.[7] This is only two more than did so in 2016.[8] Even in states where post-election audits are required, in most cases they could be far more robust. Currently, only two states, Colorado and Rhode Island, will require post-election risk-limiting audits (RLAs) in 2020 which provide "strong statistical evidence that the election outcome is right and ha[ve] a high probability of correcting a wrong outcome."[9]

Add Electronic Pollbooks to the Federal Certification Process

The existing testing and certification process put in place under the Help America Vote Act (HAVA) has significantly increased the quality and reliability of voting systems. However, over the past several years, the limitations of the current testing and certification program have become evident.

One of the biggest shortcomings has been the inability to regulate electronic pollbooks due to their lack of inclusion in HAVA. Electronic poll books (EPBs) are electronic versions of the voter rolls that are used to process voters at the polls instead of using paper-based lists. Use of EPBs

---

[7] These twenty-two states are Alaska, Arizona, California, Colorado, Connecticut, Hawaii, Illinois, Iowa, Massachusetts, Minnesota, Missouri, Montana, Nevada, New Mexico, New York, North Carolina, Ohio, Oregon, Rhode Island, Utah, Washington, and West Virginia. Although Ohio conducts post-election audits after certification, the Election Board must amend its certification if the audit results in a change of the vote totals reported in the official canvass; See "POST-ELECTION AUDITS," National Conference of State Legislatures, last modified February, 1, 2019, http://www.ncsl.org/research/elections-and-campaigns/post-electionaudits635926066.aspx; Danielle Root, Liz Kennedy, Michael Sozan, and Jerry Parshall, *Election Security in All 50 States: Defending America's Elections*, Center for American Progress, February 12, 2018, https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/.

[8] 17 R.I. Gen Laws §17-19-37.4 (2017); 2017 Iowa Acts 256.

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

has spread rapidly in the last decade, and at least 34 states as well as the District of Columbia currently use some form of EPBs to process voters at the polls.[10] One of the major benefits of EPBs is that they can make it easier to set up "vote centers" during early voting or on Election Day. Vote centers are "an alternative to traditional neighborhood-based precincts."[11] Anyone in a particular jurisdiction can vote there, regardless of where they live, possibly making voting more convenient, providing cost savings, and encouraging increased voter turnout.[12] If a county uses multiple vote centers, the electronic pollbooks can automatically sync up during the day to ensure that once someone has voted in a particular location, they cannot vote in another location on the same day.

Despite these advantages, EPBs also pose significant risks. Someone who gains unauthorized access to these pollbooks could delete names, mark individuals as felons prohibited from voting, mark individuals as having already voted, or change individuals' party affiliation to keep them from voting in a party primary.[13] Unlike voting machines, there are currently no national security standards for electronic pollbooks. Of the 34 states that have adopted them, only 13 have statewide procedures for certification requirements, or certify systems statewide, according to NCSL.[14]

HAVA's current structure limits EAC's ability to create requirements for, test, and certify EPBs in the same way they do for voting machines. The Brennan Center supports updating HAVA to allow the EAC to create a certification program for all electronic pollbooks, as they do for voting systems, in order to encourage secure EPB systems nationwide. These

[10] "VRM in the States: Electronic Poll-books," last modified February 6, 2017, Brennan Center for Justice, http://www.brennancenter.org/analysis/vrm-states-electronic-poll-books.
[11] "Vote Centers," National Conference of State Legislatures, http://www.ncsl.org/research/elections-and-campaigns/vote-centers.aspx.
[12] "Vote Centers," National Conference of State Legislatures, http://www.ncsl.org/research/elections-and-campaigns/vote-centers.aspx.
[13] Lawrence Norden and Ian Vandewalker, *Securing Elections From Foreign Interference*, Brennan Center for Justice, 2017, https://www.brennancenter.org/publication/securing-elections-foreign-interference.
[14] "Electronic Poll Books," National Conference of State Legislatures, http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx.

additional responsibilities will require increased funding and staffing levels for the EAC to effectively test and certify EPBs.

Conduct Penetration Testing and Nationwide Threat Assessments

In addition to including EPBs in the testing and certification process, the Brennan Center recommends creating an additional requirement of penetration testing for each EAC-vetted system. Penetration testing proactively identifies vulnerabilities in critical infrastructure, often by launching real-world attacks on the system. Once vulnerabilities are discovered, they are able to be addressed before malicious actors become aware of them.[15]

Periodic penetration testing of both new and existing EAC-vetted election systems should be made a routine part of the EAC certification process. This process could leverage the skills and expertise of technology companies and white hat hackers to find potential system vulnerabilities. This would ensure that our election systems are prepared to meet the challenge of defending against a landscape of new and changing cyber threats.

The Brennan Center also supports a requirement that the federal government conduct regular, nationwide threat assessments to help state and local governments understand where the vulnerabilities to cyberattack are. As cyber threats evolve, it is critical to conduct ongoing threat assessments of election infrastructure such as voter registration databases and voting systems. Conducting threat assessments on a regular basis would help state and local governments implement mitigation strategies where weaknesses are identified. In a 2017 Brennan Center report, *Securing*

[15] Meredith Berger, Charles Chretien, Caitlin Conley, Jordan D'Amato, Meredith Davis Tavera, Corinna Fehst, Josh Feinblum, Kunal Kothari, Alexander Krey, Richard Kuzma, Ryan Macias, Katherine Mansted, Henry Miller, Jennifer Nam, Zara Perumal, Jonathan Pevarnek, Anu Saha, Mike Specter and Sarah Starr, *The State and Local Election Cybersecurity Playbook*, Harvard Kennedy School and Defending Digital Democracy, 2018, 53, https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf.

Elections from Foreign Interference, we noted a consensus among experts that many states were unlikely to have completed this kind of risk assessment in the last few years, even though the cost of completing a threat assessment was likely to be manageable. In the Commonwealth of Virginia, for example, Edgardo Cortés, former Commissioner of the Virginia Department of Elections and current Brennan Center Election Security Advisor, estimates that his department could have conducted a comprehensive threat assessment or audit for just $80,000 annually.[16]

Require Private Election System Vendors to Report Cybersecurity Incidents

Private companies are contracted to perform everything from building and maintaining election websites that help voters determine how to register and where they can vote, to printing and designing ballots, to programming voting machines before each election, to building and maintaining voter registration databases, voting machines, and electronic poll books. Congress should consider additional steps to protect our elections from attacks that target these private election system vendors. Unlike other sectors that the federal government has designated "critical infrastructure," there is currently almost no federal oversight of the private vendors who build our election systems. In fact, there are more federal regulations for ballpoint pens and magic markers than there are for voting systems and other parts of our federal elections infrastructure.[17]

The Brennan Center recommends that Congress adopt a mandatory reporting system for all cyber security incidents for election vendors. While this may seem like a small step, it will have a large impact on the overall security position of election officials around the country. Election vendors have stated that such requirements are unnecessary and burdensome, and that they are somehow different from vendors in other critical infrastructure sectors. This is simply not true. We know that the lack of transparency in vendor security is a significant vulnerability to election

[16] *Securing Elections From Foreign Interference*, Brennan Center for Justice.
[17] Compare, for example, 16 C.F.R. §§ 1500.14, 1500.48, 1500.83, 1700.14, with 11 CFR §§ 9405.1 et seq.

security. Private vendors were targeted in the 2016 election and are likely to be targeted again.[18] In fact, reporting requirements for cyber security incidents are a bare minimum, and we should be considering additional requirements such as vendor employee background checks and other lessons learned from similar critical infrastructure sectors.[19] The Brennan Center has documented some of the additional reasons for mandating such reporting in the 2010 report, *Voting System Failures: A Database Solution.*[20]

Applying Cyber Security Framework to Election Systems

NIST is responsible for creating and maintaining the Cybersecurity Framework (CSF) which "consists of standards, guidelines, and practices to promote the protection of critical infrastructure."[21] The CSF assists industries, governments, and businesses in managing cybersecurity risks. In addition to the CSF, NIST creates implementation profiles that give voluntary guidance on how to adapt the CSF to particular critical infrastructure sectors. For instance, the CSF Manufacturing Profile "can be used as a roadmap for reducing cybersecurity risk for manufacturers that is aligned with manufacturing sector goals and industry best practices."[22]

NIST should prioritize the development of a CSF Elections Profile. This would be done in collaboration with other federal partners like the EAC and DHS, state election officials, local election officials, and other entities

---

[18] *Securing Elections from Foreign Interference*, Brennan Center for Justice.
[19] Brian Calkin, Kelvin Coleman, Brian de Vallance, Thomas Duffy, Curtis Dukes, Mike Garcia, John Gilligan, Paul Harrington, Caroline Hymel, Philippe Langlois, Adam Montville, Tony Sager, Ben Spear, Roisin, *A Handbook for Elections Infrastructure Security*, Center for Internet Security, February 2018, https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf.
[20] Lawrence Norden, *Voting System Failures: A Database Solution*, Brennan Center for Justice, 2010, https://www.brennancenter.org/publication/voting-system-failures-database-solution.
[21] "New to Framework," Cybersecurity Framework, National Institute of Standards and Technology, updated April 23, 2019, https://www.nist.gov/cyberframework/new-framework#background.
[22] Keith Stouffer, Timothy Zimmerman, CheeYee Tang, Joshua Lubell Jeffrey Cichonski, John McCarthy, *Cybersecurity Framework Manufacturing Profile*, National Institute of Standards and Technology, September 8, 2017, https://www.nist.gov/publications/cybersecurity-framework-manufacturing-profile.

involved in elections like election technology vendors. Implementing the Cybersecurity Framework can be a daunting task, and this profile would provide clear and direct guidance to election officials for how to best secure their systems. State and local election offices could use a CSF Elections Profile to guide prioritization of spending cyber security funds, including identifying deficiencies that need to be addressed to prevent foreign interference. This would require additional resources for NIST to develop and for the EAC to use its clearinghouse role to encourage state and local election officials to utilize the roadmap in their cybersecurity planning.

Ensuring Sufficient Funding to Protect State and Local Election Offices

Congress took an important first step in 2018 by allocating $380 million to states for election security activities. However, it is clear there is an ongoing need for federal funding to help protect our elections infrastructure from foreign threats. Congress should build on last year's efforts and provide additional funding to states to continue improving election security. Any funding should ensure that some of it is designated for use at the local level. In addition to funding for state and local election offices, Congress should ensure that federal agencies involved in this important work, including EAC, DHS, and NIST, have sufficient resources to carry out their mandates.

Conclusion

Election officials around the country need appropriate tools and resources to meet the on-going challenge of protecting our democracy from hostile nation states. We are encouraged by the great progress we have made in securing our elections since 2016, but our work in defending against cyber threats is far from complete. We urge you to consider legislative changes that will help tackle these problems head on. We appreciate this committee's leadership in continuing to strengthen our nation's election infrastructure.

Center for American Progress

1333 H Street, NW, 10th Floor
Washington, DC 20005
Tel: 202 682.1611 • Fax: 202 682.1867

www.americanprogress.org

Statement of Danielle Root, Associate Director of Voting Rights, on behalf of the Center for American Progress

For the U.S. House of Representatives Committee on Science, Space, and Technology's Subcommittee on Investigations and Oversight and Subcommittee on Research and Technology

On Election Security: Voting Technology Vulnerabilities
June 25, 2019

Chairwoman Sherrill, Chairwoman Stevens, Ranking Members Norman and Baird, and members of the House Committee on Science, Space, and Technology's Subcommittee on Investigations and Oversight and Subcommittee on Research and Technology, thank you for the opportunity to submit a statement on behalf of the Center for American Progress. The Center for American Progress is an independent nonpartisan policy institute that is dedicated to improving the lives of all Americans, through bold, progressive ideas, as well as strong leadership and concerted action.

It has now been more than two years since we first learned from intelligence officials that Russian entities attacked U.S. election infrastructure as part of an attempt to interfere in the 2016 presidential election. In addition to spreading disinformation on social media platforms, foreign actors tried to penetrate state election systems.[1] Although current evidence shows that most attacks were ultimately unsuccessful, recent reports confirm that hackers succeeded in infiltrating Illinois' voter registration database and the election systems of two counties in Florida.[2] The Special Counsel's May 2019 *Report On The Investigation Into Russian Interference In The 2016 Presidential Election* provides a comprehensive overview of Russia's attempts to influence the U.S. electoral system.

Importantly, there is still no evidence that malicious actors succeeded in manipulating voter registration data or vote counts in the 2016 election. But that will not necessarily hold true for future elections.

Cyberattacks by foreign entities and attempts to infiltrate U.S. critical infrastructure—including election infrastructure—remain a serious and persistent threat. Foreign agents are suspected to have a launched a cyberattack against the National Republican Congressional Committee in the leadup to the 2018 midterms.[3] The attack, which targeted senior NRCC aides, exposed "thousands of sensitive emails to an outside intruder."[4] And Russian agents are believed to be responsible for a series of cyberattacks against the Democratic National Committee, as well as attacks on at least one federal political campaign in 2018.[5]

In his public statement on May 29, 2019, Special Counsel Robert Mueller warned that Russia's "multiple, systematic efforts to interfere in our elections…deserve the attention of every American."[6] Director of National Intelligence Dan Coats has similarly warned that the nation's digital infrastructure is "literally under attack" and "the warning lights are blinking red again," just as they were before 9/11.[7]

Center for American Progress

1333 H Street, NW, 10th Floor
Washington, DC 20005
Tel: 202 682.1611 • Fax: 202 682.1867

www.americanprogress.org

Old voting machines and outdated equipment also pose a threat to U.S. elections. During the 2018 election cycle, voting equipment problems—such as machines jamming, stalling, and malfunctioning—plagued voting precincts in Michigan and North Carolina.[8] Polling places in New York City, as well as in South Carolina, Georgia, and Florida, also experienced problems with voting technology that caused delays and confusion.[9]

Current vulnerabilities in election technology

Since 2016, lawmakers at all levels of government have learned a great deal about the real and present danger posed by foreign interference and outdated election technology. A number of states have taken appreciable actions to fortify their election systems by adopting comprehensive reforms, including implementing cybersecurity upgrades for election technology and replacing insecure election equipment. Improved information sharing between DHS and state election administors has also helped improve the security of elections.

Despite these improvements, vulnerabilities in election technology continue to exist. A handful of jurisdictions still rely on paperless electronic voting machines that cannot be meaningfully audited to confirm election results reported by hackable machinery. In fact, a few states do not require post-election audits to be conducted at all.[10] Other jurisdictions do not test electronic poll books, which are used to check in voters, before elections to ensure they are secure and functional.[11]

In addition to threatening the integrity of our elections, problems with existing voting technology threaten the fundamental right to vote. Indeed, the right to vote cannot be exercised if the equipment used to check in voters and tabulate ballots is unreliable or malfunctions.

Of particular concern are voter registration databases, which—if successfully breached—could have a catastrophic impact on local, state, and federal races. As described previously, it is well-known that state voter registration databases were a target of Russian agents during the 2016 elections. After successfully penetrating a voter registration database, a hacker could target certain groups—such as registered Republicans or Democrats, as well as young people or individuals with different ethnic or racial backgrounds—and alter their voter registration data in ways that could prevent them from voting. For instance, simply by changing someone's registered party affiliation, a hacker could prevent a voting-eligible person from voting in a political primary. And simply by changing the spelling of someone's name, hackers could make it so that certain people are turned away at the polls. This is particularly true in states with strict voter ID requirements. Even where such hacking may not prevent a large number of Americans from actually voting, it can sow mistrust of the election system and dampen voter participation.

Voter disenfranchisement can also result from unreliable and malfunctioning election equipment. For example, during the 2018 election, potential voters left polling places in Baltimore after some electronic poll books ceased to function in the early hours of Election Day.[12] In Arizona, would-be voters were reportedly denied provisional ballots because of broken printers.[13] And in Geauga County, Ohio, some voters were denied regular ballots and were forced to vote provisionally due to a computer glitch showing they had already voted absentee.[14]

Center for American Progress

1333 H Street, NW, 10th Floor
Washington, DC 20005
Tel: 202 682.1611 • Fax: 202 682.1867

www.americanprogress.org

In an election, every single vote matters. Even small-scale cyberattacks or a few malfunctioning voting machines could determine electoral outcomes. This is especially true at a time when margins of victory are so close that elections are being decided by coin toss.[15]

For their part, election technology vendors have largely escaped accountability and calls for transparency. In 2018, it was revealed that for years, Elections Systems & Software (ES&S)—a major election technology vendor—sold machinery that contained remote-access software and internet modems, which leave equipment susceptible to hacking.[16] As described by Senator Ron Wyden (D-OR), "Installing remote-access software and modems on election equipment is the WORST decision for security short of leaving ballot boxes on a Moscow street corner."[17] It was also discovered that in 2015, the software company that maintains Maryland's voter registration platform was purchased by a company controlled by a Russian oligarch.[18] This fact was not shared with state officials until 2018, who quickly launched an investigation.[19] Members of Congress, including many members of this Committee, have already raised concerns about the lack of oversight for election technology vendors. Unfortunately, when the Senate Committee on Rules and Administration held a hearing on the subject in 2018, two of the largest vendors failed to appear for questioning.[20]

Recommendations

The 2020 presidential election is nearly upon us; primary elections will occur even sooner. Before a single vote is cast, lawmakers must act with urgency to assist states to shore up their election systems.

First, Congress must allocate additional funding to states to make necessary upgrades to election databases and equipment, and for implementing reforms, such as requiring robust post-election audits and replacing existing paperless electronic machines with paper-based voting systems. In March 2018, Congress allocated $380 million dollars for improving election security in the states.[21] Although this was a positive first step, additional funding is required. An analysis by the Brennan Center for Justice and Verified Voting found that the federal funding would not even cover the cost of replacing insecure voting machines in some states.[22] Congress should work closely with state and local officials to obtain accurate estimates for how much funding is needed to adequately secure election infrastructure across the country.

Along with additional funding, H.R.1, the "For the People Act," would go a long way to secure America's elections. H.R.1 includes several strong reforms to strengthen election infrastructure, including mandating the use of paper ballots in federal elections; providing grants to states for the purposes of carrying out risk-limiting audits; and dedicating funds towards the development of secure election equipment. H.R.1 was successfully passed in March 2019 with votes of every single Democrat in the U.S. House of Representatives but has since been stalled by Republican leadership in the Senate. Besides H.R.1, several other bills have been introduced that—if passed—would bolster the security of our elections, namely the SAFE Act (H.R.2722), which was marked up by the Committee on House Administration and is scheduled for floor action the week of June 24, 2019. The Center for American Progress strongly supports passage of the SAFE Act.

Center for American Progress

1333 H Street, NW, 10th Floor
Washington, DC 20005
Tel: 202 682.1611 • Fax: 202 682.1867

www.americanprogress.org

Furthermore, a comprehensive emergency response plan must be developed so that the nation is prepared if there is a widespread coordinated attack on federal elections or if critical infrastructure fails during voting periods. This comprehensive plan should be developed in concert with federal entities like DHS and the EAC, along with state and local representatives from the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).[23] Such a plan would help mitigate chaos and confusion if largescale problems were to occur. It would also help mitigate the potential devastating impact of systematic attacks or infrastructure failures. In doing so, it should also be made clear that foreign countries that attempt to infiltrate or wage attacks on U.S. election systems will be subject to severe penalties, which could include sanctions. An important aspect of protecting U.S. elections from foreign interference is signifying that attacks on the United States will not be tolerated.

Congressional committees should continue holding hearings about election security and inviting stakeholders across industries to provide insight and offer recommendations. This includes hearings examining election technology vendors and the role private companies play in securing election infrastructure. Members of Congress can also meet with state and local election officials, as well as voting and election security advocates, for first-hand accounts of the problems they face and the resources they need. This will help members make informed decisions about federal legislation that is responsive to on-the-ground experiences.

Finally, in developing election technology, it is crucial that technology be both highly secure and accessible for Americans with disabilities. It is particularly important for technology to allow all voting-eligible people to register to vote and have their votes counted as cast. Members of Congress should ensure legislation pertaining to election technology considers the interests and special needs of voters with disabilities.

Support for legislation to protect election infrastructure should enjoy broad bipartisan support. Election security is strictly a nonpartisan issue, a matter of national security, and core to the health of our democracy. Cyberattacks by foreign actors have been waged against Democratic *and* Republican entities. And although most attacks have so far been aimed at Democrats, this could change at any time, especially when one considers that there are other foreign governments besides Russia who have obvious interests in influencing U.S. electoral outcomes–such as China, Iran, or North Korea.

Conclusion

Concerted efforts have been made over the last two years by states and some federal entities to improve the security of the nation's election systems. But still more must be done. Vulnerabilities in election technology continue to exist, while alarming threats of cyberattacks by foreign adversaries remain ongoing. If left unaddressed, they could threaten the integrity of electoral outcomes and prevent voting-eligible Americans from casting ballots that count. The Center for American Progress applauds the Committee for addressing these issues, which remain core to America's sovereignty. The Center remains eager to assist Congress as it continues to address these critically important policy matters.

Center for American Progress

1333 H Street, NW, 10th Floor
Washington, DC 20005
Tel: 202 682.1611 • Fax: 202 682.1867

www.americanprogress.org

[1] Callum Borchers, "What we know about the 21 states targeted by Russian hackers," The Washington Post, September 23, 2017, available at https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers/?utm_term=.b032a821004b.
[2] Miles Parks, "Florida Governor Says Russian Hackers Breached 2 Counties In 2016," NPR May 14, 2019, available at https://www.npr.org/2019/05/14/723215498/florida-governor-says-russian-hackers-breached-two-florida-counties-in-2016.
[3] Jessica Taylor, "House GOP Campaign Arm Says It Was Hacked During The 2018 Election Cycle," NPR, December 4, 2018, available at https://www.npr.org/2018/12/04/673287352/house-gop-campaign-arm-says-it-was-hacked-during-the-2018-election-cycle.
[4] Alex Isenstadt and John Bresnahan, "Exclusive: Emails of top NRCC officials stolen in major 2018 hack," Politico, December 4, 2018, available at https://www.politico.com/story/2018/12/04/exclusive-emails-of-top-nrcc-officials-stolen-in-major-2018-hack-1043309.
[5] Rebecca Morin and Eric Geller, "DNC says it was target of Russia cyberattack after 2018 midterms," Politico, January 18, 2019, available at https://www.politico.com/story/2019/01/18/dnc-russia-cyberattack-midterms-1112798; Kevin Poulsen and Andrew Desiderio, "Russian Hackers' New Target: a Vulnerable Democratic Senator," The Daily Beast, October 26, 2018, available at https://www.thedailybeast.com/russian-hackers-new-target-a-vulnerable-democratic-senator.
[6] CNN Politics, "Hear Robert Mueller's Full Statement," available at https://www.cnn.com/videos/politics/2019/05/29/robert-mueller-resigns-as-special-counsel-full-statement-vpx.cnn (last accessed June 2019).
[7] Veronica Stracqualursi, "US intelligence chief: 'The warning lights are blinking red again' on cyberattacks," CNN, July 14, 2018, available at https://www.cnn.com/2018/07/14/politics/director-of-national-intelligence-dan-coats-cyberattacks-russia/index.html.
[8] Fiona Kelliher, "Voters stalled, turned away by malfunctioning voting machines," Detroit Free Press, November 6, 2018, available at https://www.freep.com/story/news/local/michigan/2018/11/06/voting-problems-issues-midterm-election-day/1901491002/; Ian McDougall and Ariana Tobin, "Long Lines Test Voter Patience Across the Nation," ProPublica, November 6, 2018, available at https://www.propublica.org/article/long-lines-test-voter-patience-across-the-nation; Dawn Baumgartner Vaughan, Aaron Moody, and Abbie Bennett, "Humidity, ballot size cause issues with voting machines in North Carolina, officials say," News and Observer, November 6, 2018, available at https://www.newsobserver.com/news/local/article221193695.html.
[9] Ian MacDougall, Jessica Huseman, and Isaac Arnsdorf, "Aging Machines, Crowds, Humidity: Problems at the Polls Were Mundane but Widespread," ProPublica, November 7, 2018, available at https://www.propublica.org/article/aging-machines-crowds-humidity-problems-at-the-polls-were-mundane-but-widespread.
[10] Danielle Root, Liz Kennedy, Mike Sozan, and Jerry Parshall, "Election Security in All 50 States: Defending America's Elections" (Washington: Center for American Progress, 2018), available at https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/.
[11] Ibid.
[12] Elizabeth Janney, "Problems At Baltimore Polls On Election Day: Missing Page, Delays," Baltimore Patch, November 6, 2018, available at https://patch.com/maryland/baltimore/vandalism-forces-polling-place-change-baltimore.
[13] MacDougall, Huseman, and Arnsdorf, "Aging Machines, Crowds, Humidity: Problems at the Polls Were Mundane but Widespread."
[14] Eric Heisig, "Computer glitch causes some Geauga County voters to be incorrectly told they voted absentee," Cleveland.com, November 6, 2018, available at https://www.cleveland.com/metro/2018/11/computer-glitch-causes-some-geauga-county-voters-to-be-incorrectly-told-they-voted-absentee.html.
[15] NPR Morning Edition, "Election Tie In Bolton, Connecticut, Decided By Coin Toss," November 17, 2017, available at https://www.npr.org/2017/11/17/564752413/election-tie-in-bolton-connecticut-decided-by-coin-toss; Trip Gabriel, "Virginia Official Pulls Republican's Name From Bowl to Pick Winner of Tied Race," New York Times, December 4, 2018, available at https://www.nytimes.com/2018/01/04/us/virginia-tie.html. See also, Tim

Center for American Progress

1333 H Street, NW, 10th Floor
Washington, DC 20005
Tel: 202 682.1611 • Fax: 202 682.1867

www.americanprogress.org

Meko, Denise Lu, and Lazaro Gamio, "How Trump won the presidency with razor-thin margins in swing states," The Washington Post, November 11, 2016, available at https://www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins/.

[16] Rachel Sandler, "Some vote-counting computers came with a critical flaw that could have let hackers access them," Business Insider, July 27, 2018, available at http://www.businessinsider.com/election-systems-and-software-admits-shipping-vote-systems-with-key-flaw-2018-7.

[17] Senator Ron Wyden (D-OR), "10:39 a.m., July 17, 2018," Twitter, available at https://twitter.com/RonWyden/status/1019275362344296451.

[18] CBS News, "Maryland told its voter registration vendor financed by Russian oligarch," available at https://www.cbsnews.com/news/maryland-voter-registration-platform-russian-oligarch/ (last accessed June 2019).

[19] Ibid. Ovetta Wiggins, "Election system firm with Maryland contract has ties to Russian oligarch, FBI tells state," Washington Post, July 13, 2018, available at https://www.washingtonpost.com/local/md-politics/marylands-election-system-tied-to-russian-oligarch-fbi-tells-state/2018/07/13/89b8ce56-86fa-11e8-8f6c-46cb43e3f306_story.html?utm_term=.386ae4701520.

[20] Senate Committee on Rules and Administration, Election Security Preparations: Federal and Vendor Perspectives, 115th Congress, 2nd sess, July 11, 2018, available at https://www.rules.senate.gov/hearings/election-security-preparations-federal-and-vendor-perspectives; Tim Starks, "Voting machine vendors under pressure," Politico, July 12, 2018, available at https://www.politico.com/newsletters/morning-cybersecurity/2018/07/12/voting-machine-vendors-under-pressure-277054.

[21] Dustin Volz, "U.S. spending bill to provide $380 million for election cyber security," Reuters, March 21, 2018, available at https://www.reuters.com/article/us-usa-fiscal-congress-cyber/u-s-spending-bill-to-provide-380-million-for-election-cyber-security-idUSKBN1GX2LC.

[22] Brennan Center for Justice and Verified Voting, "Federal Funds for Election Security: Will They Cover the Costs of Voter Marked Paper Ballots?" (2018), available at https://www.brennancenter.org/sites/default/files/analysis/Federal_Funds_for_Election_Security_analysis.pdf.

[23] National Association of County officials (NACo), "EI-ISAC protects the nation's voting infrastructure," available at https://www.naco.org/articles/ei-isac-protects-nation%E2%80%99s-voting-infrastructure (last accessed June 2019).



Statement of Verified Voting.org
Marian K. Schneider, President

United States House Committee on Science, Space, and Technology
Joint Investigations & Oversight and Research & Technology Subcommittee Hearing on
"Election Security: Voting Technology Vulnerabilities"
Subcommittee on Investigations and Oversight
Subcommittee on Research and Technology

June 25, 2019

2:00 pm Rayburn House Office Building, Washington, DC

Chairwoman Sherrill, Ranking Member Norman, Chairwoman Stevens, Ranking Member Baird and committee members, thank you for the invitation to submit a written statement in connection with the Joint Investigations & Oversight and Research & Technology Subcommittee Hearing on "Election Security: Voting Technology Vulnerabilities." Our statement will focus on 1) a brief overview of technologies in use for election administration; 2) describe some of the risks associated with those technologies as well as solutions for mitigating those risks; 3) review the role that NIST and other agencies have played in developing technologies for secure elections; and 4) suggest regulatory changes necessary to address advances in voting technology and the changing threat model facing our elections.

The scale and scope of threats to U.S. elections go far beyond what the current federal policy framework can address. Since the Help America Vote Act was passed, technology has advanced and the security threat landscape has also evolved. It's time to re-think the regulatory framework to align it with the current environment. Your committee plays a crucial role in shaping our collective response. We urge the committee to take the steps necessary to enact mandatory security measures for all technology that touches election administration, to ensure that the foundation of our democracy is protected from ongoing threats.

About Verified Voting

Verified Voting's mission is to strengthen democracy by promoting the responsible use of technology in elections. Since our founding in 2004 by Stanford computer science professor David Dill, we have acted on the belief that the integrity and strength of our democracy relies on citizens' trust that each vote is counted as cast. Our board of directors and board of advisors

include some of the top computer scientists, cyber security experts and statisticians working in the election administration arena as well as former and current elections officials. We bring together policymakers and officials who are designing and implementing voting-related legislation and regulations with technology experts who comprehend the risks associated with election technology. We have provided direct assistance to election officials in implementing the most efficient post-election audits to verify election results. Additionally, we connect advocates and researchers, the media, and the public to provide greater understanding of these complex issues.

The Scope of the Problems with Election Security and Current Election Infrastructure

Election administration depends on computers at multiple points in the election process. Equipment for the actual act of voting is but one part of a broad array of election technology infrastructure that supports the conduct of elections today. Some of that technology infrastructure includes voter registration databases, internet facing applications such as online voter registration and polling place lookup, network connections between state government and local jurisdictions, the computers that program the voting devices that record and count votes in addition to the voting devices themselves. Some jurisdictions also use electronic poll books to check voters in at polling sites and most states and localities report election night returns via a website.

To the extent that any of these can be compromised or manipulated, can contain errors, or can fail to operate correctly -- or at all -- this can potentially affect the vote but may also affect the public perception of a fair and accurate election. Election system security requires not only efforts to prevent breaches and malfunctions, but also fail-safes that remedy breaches and malfunctions that do occur.

Limitations of the Current Federal Policy Framework

The U.S. federal policy framework is not designed to ensure -- or even address -- the security of this complex and varied election infrastructure. U.S. elections are administered by state, county, and in some cases municipal officials. The Help America Vote Act of 2002 (HAVA) broke new ground by establishing the Election Assistance Commission. The EAC has very little regulatory authority, but it is tasked (inter alia) with adopting Voluntary Voting System Guidelines (VVSG), developed in collaboration with the National Institute of Standards and Technology (NIST), and with certifying systems under those standards. Although the VVSG is voluntary, many states require their own voting systems to be certified under the standards. The VVSG applies only to voting systems. The EAC can address other parts of election infrastructure in its role as a clearinghouse for election administration information, but has limited resources for doing so. Neither the EAC nor any other federal agency or department has



ever been given clear responsibility and resources directed toward countering persistent and coordinated cyber attacks on election systems. In the past, state and local officials have not been trained or funded to thwart cyber attacks on our election system let alone attacks coordinated by another nation state. Yet that is the threat our nation confronts.

Since the 2016 election, and as a result of the national security community warnings that the potential for attacks against our election infrastructure is real and ongoing, federal agencies have launched new initiatives to work with state and local governments and election officials to increase the understanding of cyber security threats to elections, to prepare election offices to address the threat and provide the tools to recover from breaches should they occur.[1] The DHS-funded Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) has facilitated timely communication about threat mitigation. Other organizations and groups have also worked to provide best practices for security of election assets by publishing handbooks and guides.[2] State and local election offices have also engaged in "table top" exercises to simulate real-time election day incidents and practice incident response process in advance of a cyber security event. These efforts are a welcome change of relatively recent vintage. But, for local election officials to be better prepared, they need resources to continue the existing efforts and ongoing training, even with the support that DHS currently offers. As we discuss below, technology touches election administration in numerous places and the use of technology requires additional resources to ensure the validity of the election.

Despite considerable progress in the last few years, much work must be done to secure our nation's elections infrastructure. Two primary areas that require immediate and sustained attention are 1) securing both the state and county networks, databases, and data transmission infrastructure that touch elections; and 2) instilling confidence in election outcomes by replacing older, vulnerable legacy voting systems with new systems that permit reliable and robust post election audits and recounts.

Voter Registration Databases

Under the Help America Vote Act, states were required to adopt "a single, uniform, official, centralized, interactive computerized statewide voter registration list defined,

---

[1] *See e.g.*, Department of Homeland Security, the Cybersecurity and Infrastructure Security Agency (CISA), for a summary of its work with Elections Officials, through its program "#Protect2020" available here: https://www.dhs.gov/cisa/protect2020

[2] Handbook for Elections Infrastructure Security, Version 1.0." the Center for Internet Security, February 2018, Retrieved from: https://www.cisecurity.org/elections-resources/; "The State and Local Election Cybersecurity Playbook," Belfer Center for Science and International Affairs, Harvard Kennedy School, February 2018. Retrieved from: https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook#practices.



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."[3] Those databases are usually stored on the state's network and are accessed by the local jurisdictions who have authority to register voters.

These systems face substantial security threats. Statewide voter registration databases are connected to localities and other agencies via networks, potentially exposing them to attack. Likewise, internet-facing applications and tools that touch voter registration present their own set of risks to the integrity of the voter registration rolls because they are connected to the Internet. Finally, complete and accurate voter registration lists must be available at the polling place. When jurisdictions choose electronic pollbooks to check voter registration status and sign voters in, these e-pollbooks become another target. We further discuss this threat below.

The cybersecurity risks presented by network-connected voter registration databases are no different than similar risks presented by other databases that contain mission critical data and personally identifying information. According to the U.S. Department of Homeland Security, voter registration databases are vulnerable to a variety of attacks using an equal variety of methods. These can include direct web-based attacks that seek to inject or send commands to enable the attacker to gain unauthorized access to information; denial of service attacks that prevent legitimate users from being able to use election information or services; ransomware attacks that block legitimate users' access to a system until a ransom is paid; and more. Phishing attacks involve forged emails or other messages designed to get the recipient to click on malicious links or otherwise provide an entry point for stealing credentials such as passwords, spread malware or disrupt voting operations.[4]

Although the Help America Vote Act required states to centralize voter registration databases, mainly to provide a more uniform experience for voters rather than relying on a patchwork of systems that varied widely within a state, that statute did not contemplate the advances in technology or the evolving threats directed to those technologies. For example, HAVA does not regulate online voter registration applications or automatic voter registration systems but those are becoming increasingly widespread. Moreover, the creation and deployment of voter registration systems varies from custom-created in-house, to vendor-supplied, to commercial software packages that can be configured.

---

[3] Help America Vote Act, 52 U.S. Code § 21083.

[4] "Securing Voter Registration Data." National Protections and Programs Directorate, Department of Homeland Security, June 26, 2018. Retrieved from https://www.dhs.gov/sites/default/files/publications/Securing%20Voter%20Registration%20Data_0.pdf;



In the consensus study report "Securing the Vote" the National Academies of Sciences, Engineering and Medicine found that voter registration databases are subject to cybersecurity vulnerabilities and attacks. In addition, because such databases contain personally identifying information, significant harm could occur if such databases were breached.[5] The National Academies recommended routine assessment of voter registration databases that would allow jurisdictions to detect any tampering or interference with the database. We support that recommendation. To implement it, states and localities need the appropriate resources to conduct such assessments. Federal support is warranted to address these threats to national elections. Moreover, it is imperative that a regulatory framework or guideline be developed by NIST or an agency with cyber security expertise, against which such voter registration systems could be examined or audited.

Electronic poll books

Electronic poll books (EPBs) are computerized and usually networked devices that substitute for paper lists of voters in a polling place. These EPBs serve several useful functions for checking voter status, checking voters in to vote, enabling poll workers to guide voters to a different location if needed, and more. The spread of electronic poll books has been significant in recent years; 34 states are currently using EPBs in some or all jurisdictions.

The correct functioning of such devices is crucial and can affect voters' ability to cast an effective ballot. Because electronic poll books rely on communications connectivity that must function in real-time on Election Day, failure of such devices can result in late-opening polling places and disenfranchisement of voters who cannot wait for a paper back-up to arrive, or who may not be offered a failsafe provisional ballot. In their Preliminary Report on the 2018 Midterm Elections, the Election Protection Coalition reported that among other technology issues affecting voters, there were numerous instances of "broken voter check-in machines or e-poll books which prevented or slowed the voting process[....] In the most severe cases, faulty or insufficient equipment caused hours-long delays and resulted in many voters being unable to vote."[6] Recently the Department of Homeland Security announced it would conduct forensic investigation of EPBs that caused significant problems in North Carolina in 2016[7], after it was revealed that systems of the company providing the EPBs had been breached in another state.

---

[5] "Securing the Vote: Protecting American Democracy." The National Academies of Sciences, Engineering and Medicine, Consensus Study Report, September, 2018 at 63.

[6]https://lawyerscommittee.org/wp-content/uploads/2018/12/Election-Protection-Preliminary-Report-on-the-2018-Midterm-Elections.pdf

[7]https://www.washingtonpost.com/investigations/federal-investigators-to-examine-equipment-from-2016-north-carolina-election-amid-renewed-fears-of-russian-hacking/2019/06/05/b70402e6-7816-11e9-b7ae-390de4259661_story.html?utm_term=.93292ced5c5b

Despite the risks inherent in using computerized networked systems for checking in voters, there are no national standards for electronic poll books, and most states using them do not require a certification process. Some states conduct testing and certification, yet even those standards vary from state to state and may not be sufficient.

An important mitigation where EPBs are deployed is to provide paper poll books in case of EPB system failures, and a sufficient quantity of provisional ballots to issue when needed, so that the flow of voters at the polling place will not be unduly interrupted. Election officials also may avail themselves of risk and vulnerability assessments (RVA), remote penetration testing and vulnerability scans, provided by the Cybersecurity and Infrastructure Security Agency (CISA) of DHS.

However, additional structural fixes are needed if such systems are to be used safely. In the consensus report "Securing the Vote," the National Academies found that "Congress should authorize and fund the National Institute of Standards and Technology, in consultation with the U.S. Election Assistance Commission, to develop security standards and verification and validation protocols for electronic pollbooks in addition to the standards and verification and validation protocols they have developed for voting systems."

The report further found that "election administrators should routinely assess the security of electronic pollbooks against a range of threats such as threats to the integrity, confidentiality, or availability of pollbooks. They should develop plans that detail security procedures for assessing electronic pollbook integrity."

Both are sound recommendations. As with voting registration databases, we recommend ensuring that election officials have the necessary resources to carry out these assessments.

Electronic Voting Systems

Fortunately, for voting systems, a general consensus has formed on the steps necessary to provide a secure, reliable and verifiable election:

- A paper ballot (marked by pen or computerized ballot marking device) that voters can verify before casting;
- Routine, robust post-election audits to either confirm that reported outcomes are accurate or identify problems for further investigation before vote counts are finalized; and
- The ability to carry out full manual recounts if needed.



For technology used for marking and counting votes, voters must be able to confirm first-hand that their ballots were indeed marked as they intended, and election officials must be able to use those ballots to demonstrate that all the votes were included and were counted as cast. This process is crucial to defuse the narrative that our elections can be hacked.

Since 2016, the percentage of states with some form of paper record has increased from 70% to 77%. While that progress is laudable, the movement towards effective post-election tabulation audits that would confirm that the software-reported results are correct has occurred much more slowly. In addition, there has been no comprehensive regulatory oversight of whether commercially available options actually facilitate effective post-election audits. Are the voting devices on the market designed to ensure that voters verify that their choices are correct? Are all voters able to verify their votes without relying on the voting system itself? Is the record that is preserved a trustworthy artifact of voter intent? To the extent that system design, software configuration, hardware design or other factors interfere with the preservation of a trustworthy record, the utility of post-election audits is undermined.

The Role of Science Agencies in Standards-Setting, Research and Development

Under the Help America Vote Act, the National Institute of Standards and Technology (NIST) functions as an independent team of expert advisors, giving technical guidance to the Election Assistance Commission in particular for the development of the Voluntary Voting System Guidelines (VVSG). NIST further has published guidance on topics relevant to electoral systems, including several on security best practices for remote electronic voting and materials transmission for military and overseas voters.[8] Those publications contain crucial information about best practices in the use of various computer and communications technologies to support secure elections. However, this work has insufficient impact. None of NIST's guidance is mandatory. NIST's recent collaboration with EAC and with stakeholders in the development of the newest VVSG draft helped to profoundly change and improve how those principles and guidelines are generated, thinking beyond just voting systems to the broader election context, but the guidelines nonetheless are limited to the narrow focus of voting systems.

With additional funding, NIST has the potential and technical expertise to provide much more than it does today, whether independently or in collaboration with the EAC. For example, it could readily develop guidelines against which voter registration systems, electronic poll books and even election night reporting systems should be tested, even absent EAC oversight of such a testing function. Such guidelines would help states' election administrators to ensure they are taking all the steps necessary to safeguard those critical systems and reduce the likelihood

[8] https://www.nist.gov/itl/voting/publications



and impact of foreign interference or other tampering, as well as problems caused by malfunctions. Congress could make such guidelines mandatory, or at a minimum, create incentives for states to adhere to them.

NIST could also assist in developing standards for post-election audits and the emerging systems used to support the conduct of audits. The conduct of rigorous audits is essential to ensuring reliable election outcomes and voter confidence; no amount of voting system testing or certification can substitute for this process. While NIST has provided valuable insight through its Auditability Working Group[9], it could further support this critical process. These additional tasks for NIST can succeed because NIST has the ability to leverage its considerable scientific expertise to tackle these problems.

Two other science agencies, the Defense Advanced Research Projects Agency (DARPA) and the National Science Foundation (NSF), have a significant impact on electoral systems and security by funding research and development of systems and methods that can improve election security, and could do more with directed initiatives and sufficient funding. The Defense Advanced Research Projects Agency (DARPA) has granted an award of $10 million to Galois, Inc. for open source development of two demonstration voting systems on a secure software platform, one a ballot marking device and the other a ballot scanning device that counts votes from the scanned ballots.[10] Such initiatives are crucial because election system vendors, operating in a niche market, have not demonstrated the ability to innovate for excellence in election security and usability. Federal research and development support can produce new designs and software solutions that vendors can incorporate in their systems or pave the way for publicly-owned open source solutions that might have significant cost savings for governments. All of this work supporting the sound science behind election security should proceed in coordination with DHS' own efforts in this regard and with EAC's work on election administration.

The National Science Foundation (NSF) engagement in funding studies and investigations into various aspects of voting system security has been extremely valuable, but not constant. Some past examples include a 1999 study on Internet voting[11]; a multi-year initiative starting in 2005 for "A Center for Correct, Usable, Reliable, Auditable and Transparent Elections" (ACCURATE)[12]; a 2007 grant for developing an open source system called Prime III[13]; grants in 2014 for studying open audit voting systems and protocols[14]; and a grant starting

[9] https://www.nist.gov/document-7152
[10] https://defensesystems.com/articles/2019/03/18/darpa-secure-voting.aspx
[11] https://www.nsf.gov/od/lpa/news/press/01/pr0118.htm
[12] https://www.nsf.gov/news/news_summ.jsp?cntn_id=111660
[13] https://www.nsf.gov/awardsearch/showAward?AWD_ID=0738175
[14] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1421373



in 2015 for studying the threats to election integrity deriving from poor ballot usability[15], among others. These examples illustrate the potential for scientific initiatives to support improvements in U.S. voting technology. Election security is not a one-time challenge; it warrants ample and sustained research investment.

Recommendations for Modernizing the Regulatory Framework around Election Security

In summary, we see both immediate needs to bolster public investment in the science of election security, and a broader need to rethink the policy framework that shapes our national response to election security threats.

- Standards-setting must extend beyond voting systems to other election technologies, including voter registration databases, electronic pollbooks, and election reporting systems. With statutory support and funding, NIST is well positioned to lead these efforts as it has led the ambitious effort to update the Voluntary Voting System Guidelines.
- NIST and other agencies should receive ample funding to add additional highly qualified staff, to support standards-setting work and to inform policymakers and election administrators.
- NSF and other agencies should be fully funded to invest in research and development into election security threats and mitigations.
- Broader deliberation is needed on how best to adapt the HAVA framework to today's election security challenges. The various roles of DHS, EAC, NIST, DARPA, NSF, and other agencies are not always clearly defined, and nothing in current law addresses many of the threats we have discussed here. It is easy to recommend that all these agencies should receive more funding for their election protection work -- but how should the work be divided and coordinated? We would like to see a blue-ribbon panel specifically study the policy questions of interagency coordination on election security, taking into account the need for cooperation with state and local policymakers and officials.

[15] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1550936

Common Cause
Holding Power Accountable

805 Fifteenth Street NW, Suite 800
Washington, DC 20005
202.833.1200
www.commoncause.org

U.S. House Committee on Science, Space, and Technology
Subcommittee on Investigations and Oversight
Subcommittee on Research and Technology
Joint Hearing on:
"Election Security: Voting Technology Vulnerabilities"
2318 Rayburn House Office Building, Washington, DC
June 25, 2019

Written Statement of
Karen Hobert Flynn
President
Common Cause

Dear Chairwoman Sherrill and Chairwoman Stevens:

On behalf of Common Cause's 1.2 million members around the country, we write to commend you for holding this critical hearing entitled, "Election Security: Voting Technology Vulnerabilities". According to the leaders of the U.S. intelligence community, Russia and other hostile foreign entities continue to try to interfere in our elections, and we must do everything we can to protect our democracy against these attacks. Although Congress appropriated $380 million to the states last year, this appropriation is simply not enough to help state and local election officials make the necessary cyber security upgrades they need to defend themselves against sophisticated nation-state actors.

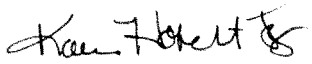
We also know from the published research of experts from National Institute for Standards and Technology (NIST) and the National Academies of Sciences, Math and Engineering recent report entitled *Securing the Vote : Protecting American Democracy* that there are necessary changes we must make to our election infrastructure to ensure that it is resilient in the face of an attack. We need:

- All voting systems to produce a voter verifiable paper ballot. Paper ballots are a critical failsafe. If vote tallies are corrupted for any reason, the paper ballots can be used to ascertain the true result. This is a low-tech deterrent to the attempt to tamper with the final vote count by introducing sophisticated malware into the vote tallying system;
- All states to conduct risk limiting post-election audits of their election contests. A grant program should be established so that states have necessary resources and training to conduct these audits. This type of audit ensures that the results of the election are correct. Risk limiting audits are the only type of audit that checks election outcomes to a very high confidence level; they are critical to giving us the evidence to know that the winner really won;

- Vendors to swiftly report cybersecurity breaches and other cybersecurity incidents; vendors should not be able to withhold knowledge of a breach from the election administrators that depend on their products;
- Vendors to certify their systems to the latest Voluntary Voting System Guidelines (VVSG) and to make source code available for inspection by the public; and
- States to certify that they have adopted cyber security best practices in the maintenance of their statewide voter registration databases.

Thank you for holding this critical hearing. We look forward to continue working to ensure the integrity of our elections so that all Americans can have confidence that their ballots are counted as cast.

Sincerely,



Karen Hobert Flynn
President
Common Cause

National Election Defense Coalition

Chairwoman Eddie Bernice Johnson
Ranking Member Frank Lucus
Subcommittee on Investigations & Oversight
House Committee on Science, Space & Technology
4212 O'Neill House Office Building
Washington, DC

June 24, 2019

Dear Chairwoman Johnson and Ranking Member Lucus,

Thank you very much for holding a hearing on Election Security: Election Technology Vulnerabilities. The National Election Defense Coalition (NEDC) is a non-partisan, not-for-profit organization that advocates for policies and practices to secure election systems. NEDC seeks to act as a bridge between election stakeholders and policy-makers on the right and left; and between computer security experts and election administrators and lawmakers. We thank you for the opportunity to provide a statement on "Election Security: Election Technology Vulnerabilities."

In 2016 we learned the chilling reality that foreign agents were actively trying to attack our election infrastructure through cyber attacks. In the last three years the warnings have not abated; instead our intelligence agencies have issued increasingly urgent warnings that our elections are being targeted for manipulation. Though these attacks can take many forms - including the manipulation of social media to influence public perception - NEDC focuses on election system technology, vulnerabilities, and security. While we will limit our comments to attacks on election infrastructure, we do not mean to minimize the influence, damage or seriousness of social media attacks.

Our election systems today are dependent on computers. Computers, by nature, are susceptible to cyber attacks which means our elections are vulnerable to manipulation through cyber attacks. We recognize two segments of the election system as primary targets for adversaries aiming to disrupt, de-legitimize and/or tamper with our elections: 1) the voter registration system, 2) the vote recording and tabulating systems.

1. The Voter Registration System: The voter registration system functions to manage the voter registration records of all eligible voters within the State. This will include a state-wide voter registration database as well as the individual county databases. In states that use electronic pollbooks to digitally store voter records and check voters in to the polls when they vote, electronic pollbooks are also part of the voter registration system.

   An attacker could tamper with elements of the voter registration system to cause either widespread disruption or selective disenfranchisement of voters by political party, race or residence. By destroying a voter registration database or altering or deleting voter registration records on a large scale an attacker could cause mass chaos on Election Day. The corrupted

voter registration database would force countless eligible voters to vote provisional ballots rather than regular ballots, creating lines, stressing poll workers, overwhelming the system, and diminishing confidence in the election process. If the original voter registration database is corrupted, it will be difficult if not impossible to correctly adjudicate, cure and count the provisional ballots potentially disenfranchising numerous voters.

An attacker could also launch a more surgical and targeted attack designed to disenfranchise selected voters based on the voters' political leanings without creating the chaos that might signal there has been an attack on the voter registration records. Once the attackers have access to the voter registration system they could selectively remove or alter voters' records based on their race, residence, or political party forcing eligible voters to vote provisionally. Again, if the master voter registration database is corrupted it may not be possible to properly adjudicate the provisional ballots, effectively disenfranchising eligible voters. Furthermore, the act of forcing eligible voters to vote provisionally will cause wait times that some voters will be unable to tolerate, resulting in voters leaving without casting a ballot. By altering voter registration records of voters based on their political leanings, an attacker could hack of a voter registration system to tamper with an election in favor of one candidate or party over another in a form of "digital voter suppression." Additionally, hackers could also target the vendors that provide or service voter registration systems and/or epollbooks in order to access and corrupt voter registration records.

These scenarios are less theoretical than one might hope. In 2016 it was revealed that hackers attacked voter registration systems in Arizona and Illinois.[1] Since then we have learned that foreign hackers likely tried to hack election systems in all fifty states[2] and breached a vendor, VR Systems.

VR Systems provided voter registration systems and epollbooks to several states in 2016 including Durham County, NC. On Election Day 2016 Durham County experienced severe malfunctions of its epollbooks, compelling the County to cease using the epollbooks and switch to paper pollbooks. The North Carolina State Board of Elections acknowledged that it did not have the resources or expertise to establish if the epollbooks' failures were connected to the cyber attack on the epollbook vendor VR Systems.[3] Only recently did North Carolina's election administration ask the Department of Homeland Security to examine the system.[4] It's still unknown if there is a connection between the attack on VR Systems and the epollbook failure in Durham, NC on Election Day 2016.

2. Vote Capture and Tabulation Systems: Hackers can also target the actual systems that record and tabulate votes. These systems are particularly vulnerable to undetectable

[1] Ellen Nakashima, "Russian hackers targeted Arizona Election System," *The Washington 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?utm_term=.121eab81fa9a

[2] Sean Gallagher, "DHS, FBI say election systems in all 50 states were targeted in 2016," *ArsTechnica,* Apr. 10, 2019 https://arstechnica.com/information-technology/2019/04/dhs-fbi-say-election-systems-in-50-states-were-targeted-in-2016/

[3] Will Doran, "Did Russian spies hack NC voting software? Mueller report adds to suspicions," *The News and Observer,* Apr. 19, 2019 https://www.newsobserver.com/news/politics-government/article229460734.html

[4] Pam Fessler, "Federal Government to Inspect North Carolina Election Equipment Over Hacking Fears," *NPR,* Jun 5, 2019. https://www.npr.org/2019/06/05/729920147/federal-government-to-inspect-north-carolina-election-equipment-over-hacking-fea

manipulation because we vote by secret ballot; once the ballot is cast, it's not possible for the voter to confirm that her ballot has been cast and counted as intended. For this reason, computer security experts from both the private sector and the National Institute of Standards and Technology (NIST) have long warned that it is critical that an election system provide a voter-verified paper ballot that can be used to audit election results to ensure the totals are correct.[5] The voter-verified paper ballot provides a physical (not digital) record of voter intent that enables the voter to confirm her vote is recorded correctly. The paper ballot can then be used to check the digital results to ensure they are accurate. The most effective and efficient way to provide voter-verified paper ballots is to utilize hand-marked paper ballots and offer assistive technology for voters that may need assistance marking a paper ballot privately and independently.

This means that a voter-verified paper ballot and post-election audit are absolutely essential to ensure election results are correct. Other security precautions can and should be in place but it's critical to recognize that highly skilled nation-state attackers could defeat common safeguards, successfully corrupt voting systems and undetectably alter votes and election results.

Briefly we will explain the limitations of some of the more frequently cited security measures to understand the necessity of paper ballots and post-election audits.

A) "Voting machines are not connected to the Internet." This is the most frequently repeated myth regarding voting system security and is misleading on two levels. First, even if voting machines are not directly connected to the internet they are still vulnerable to remote cyber attacks that can effected by infecting the legitimate programming files that must be transmitted to the voting machines though flash drives or other media.[6] Secondly, many voting machines have built-in wireless modems that are used to transmit election results at the close of polls to the County for aggregation. Even if the wireless modems are only turned on at the end of voting for a brief time and are configured not to receive data, they can still be compromised, providing an online attack vector directly to the voting system.[7]

B) "Voting systems are decentralized." It's correct that voting systems are highly decentralized in the U.S. but it's faulty to conclude this serves as a security safeguard. It is now widely recognized that decentralization fails to provide greater security for national or even local elections. An attacker need only target one or two key counties in just a few swing states to impact a national election. At a hearing of the Senate Select Committee on Intelligence, both former

[5] National Institute of Standards and Technology, "Report of the Auditability Working Group," https://www.nist.gov/document-7151
[6] Kim Zetter, "The Myth of the Hacker-Proof Voting Machine," *The New York Times,* Feb. 21, 2018
https://www.nytimes.com/2018/02/21/magazine/the-myth-of-the-hacker-proof-voting-machine.html
[7] Experts letter to DHS and EAC on wireless modems in voting machines. https://www.electiondefense.org/letter-to-eac-and-dhs/

Secretaries of the Department of Homeland Security, Jeh Johnson and Kirstjen Nielsen, refuted this notion. As Secretary Nielsen stated:

"[Decentralization…makes it perhaps of greater threat at a local level. If it's a swing state or swing area, that can, in turn, have a national effect."[8]

C) "Voting systems undergo pre-election testing." Pre-election testing is a critical and necessary measure for election administration but it has limited value as a safeguard against hacking. This is because a sophisticated hacker would likely design his/her attack to lie dormant during testing and only kick-in during the election. Computer security experts have warned for years that malicious software can be designed to be undetectable during testing. This was most famously illustrated by the malicious software designed to cheat emissions tests for Volkswagon cars.[9]

This is why it is essential that election systems utilize a voter-verified paper ballot and conduct robust, post-election audits designed to detect and correct corrupted or incorrect election results to secure our elections.

It's important to note that though over half the states may conduct some sort of post-election audit, only a few of these are actually designed to detect and correct an incorrect error in an election outcome. For example, Pennsylvania, Texas and New Jersey all have post-election audit laws but most of the counties in these states don't yet have paper ballots-which means that a post-election audit cannot be meaningfully conducted to detect and correct errors in the election outcome. In other states the post-election audit is conducted after the election is certified which means it is useless as a security safeguard to protect against a corrupted outcome. In order to protect our elections, we need post-election audits that are specifically designed to serve as a security measure; to detect and correct a corrupted election outcome.

Though states are recognizing the importance of securing voter registration systems, adopting voter-verified paper ballots and conducting robust post-election audits, the adoption of these measures has been slow. Federal legislation is necessary to compel the universal adoption of these essential security measures. As the Subcommittee explores this issue further, we welcome the opportunity to provide additional information and answer any questions you may have.

Thank you very much for the opportunity to submit this statement and we stand ready to assist you in anyway we can.

Sincerely,

Susan Greenhalgh
Policy Director
National Election Defense Coalition

---

[8] Miles Parks, "Congress Set To Approve Nearly $700 Million For Election Security, Source Says," *National Public Radio,* March 21, 2018
[9] Russell Holten, "Volkswagon: The scandal explained," *BBC,* Dec. 10, 2015 https://www.bbc.com/news/business-34324772

DOCUMENT SUBMITTED BY REP. SEAN CASTEN

U.S. Department of Justice
~~Attorney Work Product~~ // ~~May Contain Material Protected Under Fed. R. Crim. P. 6(e)~~

Report On The Investigation Into Russian Interference In The 2016 Presidential Election

Volume I of II

Special Counsel Robert S. Mueller, III

Submitted Pursuant to 28 C.F.R. § 600.8(c)

Washington, D.C.

March 2019

them to [redacted] account that they controlled; from there, the copies were moved to GRU-controlled computers. The GRU stole approximately 300 gigabytes of data from the DNC cloud-based account.[185]

2. Intrusions Targeting the Administration of U.S. Elections

In addition to targeting individuals involved in the Clinton Campaign, GRU officers also targeted individuals and entities involved in the administration of the elections. Victims included U.S. state and local entities, such as state boards of elections (SBOEs), secretaries of state, and county governments, as well as individuals who worked for those entities.[186] The GRU also targeted private technology firms responsible for manufacturing and administering election-related software and hardware, such as voter registration software and electronic polling stations.[187] The GRU continued to target these victims through the elections in November 2016. While the investigation identified evidence that the GRU targeted these individuals and entities, the Office did not investigate further. The Office did not, for instance, obtain or examine servers or other relevant items belonging to these victims. The Office understands that the FBI, the U.S. Department of Homeland Security, and the states have separately investigated that activity.

By at least the summer of 2016, GRU officers sought access to state and local computer networks by exploiting known software vulnerabilities on websites of state and local governmental entities. GRU officers, for example, targeted state and local databases of registered voters using a technique known as "SQL injection," by which malicious code was sent to the state or local website in order to run commands (such as exfiltrating the database contents).[188] In one instance in approximately June 2016, the GRU compromised the computer network of the Illinois State Board of Elections by exploiting a vulnerability in the SBOE's website. The GRU then gained access to a database containing information on millions of registered Illinois voters,[189] and extracted data related to thousands of U.S. voters before the malicious activity was identified.[190]

GRU officers [redacted] scanned state and local websites for vulnerabilities. For example, over a two-day period in July 2016, GRU officers [redacted] for vulnerabilities on websites of more than two dozen states. [redacted]

[185] *Netyksho* Indictment ¶ 34; *see also* SM-2589105-HACK, serial 29 [redacted].

[186] *Netyksho* Indictment ¶ 69.

[187] *Netyksho* Indictment ¶ 69; [redacted]

[188] [redacted]

[189] [redacted]

[190] [redacted]

[redacted]

Similar [redacted] for vulnerabilities continued through the election.

Unit 74455 also sent spearphishing emails to public officials involved in election administration and personnel at companies involved in voting technology. In August 2016, GRU officers targeted employees of [redacted], a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network. Similarly, in November 2016, the GRU sent spearphishing emails to over 120 email accounts used by Florida county officials responsible for administering the 2016 U.S. election.[191] The spearphishing emails contained an attached Word document coded with malicious software (commonly referred to as a Trojan) that permitted the GRU to access the infected computer.[192] The FBI was separately responsible for this investigation. We understand the FBI believes that this operation enabled the GRU to gain access to the network of at least one Florida county government. The Office did not independently verify that belief and, as explained above, did not undertake the investigative steps that would have been necessary to do so.

D. Trump Campaign and the Dissemination of Hacked Materials

The Trump Campaign showed interest in WikiLeaks's releases of hacked materials throughout the summer and fall of 2016. [redacted]

1. [redacted]

a. Background

[redacted]

[191] *Netyksho* Indictment ¶ 76; [redacted]

[192] [redacted]