PROTECTING THE 2016 ELECTIONS FROM CYBER AND VOTING MACHINE ATTACKS

HEARING

BEFORE THE

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

September 13, 2016

Serial No. 114–91

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
22–560PDF WASHINGTON : 2017

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

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

FRANK D. LUCAS, Oklahoma
F. JAMES SENSENBRENNER, JR., Wisconsin
DANA ROHRABACHER, California
RANDY NEUGEBAUER, Texas
MICHAEL T. MCCAUL, Texas
MO BROOKS, Alabama
RANDY HULTGREN, Illinois
BILL POSEY, Florida
THOMAS MASSIE, Kentucky
JIM BRIDENSTINE, Oklahoma
RANDY K. WEBER, Texas
JOHN R. MOOLENAAR, Michigan
STEVE KNIGHT, California
BRIAN BABIN, Texas
BRUCE WESTERMAN, Arkansas
BARBARA COMSTOCK, Virginia
GARY PALMER, Alabama
BARRY LOUDERMILK, Georgia
RALPH LEE ABRAHAM, Louisiana
DARIN LAHOOD, Illinois
WARREN DAVIDSON, Ohio

EDDIE BERNICE JOHNSON, Texas
ZOE LOFGREN, California
DANIEL LIPINSKI, Illinois
DONNA F. EDWARDS, Maryland
SUZANNE BONAMICI, Oregon
ERIC SWALWELL, California
ALAN GRAYSON, Florida
AMI BERA, California
ELIZABETH H. ESTY, Connecticut
MARC A. VEASEY, Texas
KATHERINE M. CLARK, Massachusetts
DON S. BEYER, JR., Virginia
ED PERLMUTTER, Colorado
PAUL TONKO, New York
MARK TAKANO, California
BILL FOSTER, Illinois

CONTENTS

September 13, 2016

	Page
Witness List	2
Hearing Charter	3

Opening Statements

Statement by Representative Lamar S. Smith, Chairman, Committee on Science, Space, and Technology, U.S. House of Representatives	5
Written Statement	7
Statement by Representative Eddie Bernice Johnson, Ranking Member, Committee on Science, Space, and Technology, U.S. House of Representatives	9
Written Statement	11

Witnesses:

Dr. Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology	
Oral Statement	14
Written Statement	17
Hon. Tom Schedler, Secretary of State, State of Louisiana	
Oral Statement	27
Written Statement	29
Mr. David Becker, Executive Director, The Center for Election Innovation & Research	
Oral Statement	35
Written Statement	38
Dr. Dan S. Wallach, Professor, Department of Computer Science and Rice Scholar, Baker Institute for Public Policy, Rice University	
Oral Statement	42
Written Statement	44
Discussion	56

Appendix I: Answers to Post-Hearing Questions

Dr. Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology	88
Hon. Tom Schedler, Secretary of State, State of Louisiana	107
Mr. David Becker, Executive Director, The Center for Election Innovation & Research	110
Dr. Dan S. Wallach, Professor, Department of Computer Science and Rice Scholar, Baker Institute for Public Policy, Rice University	113

Appendix II: Additional Material for the Record

Washington Post article *How to hack- and rig-proof U.S. elections*	122

PROTECTING THE 2016 ELECTIONS FROM CYBER AND VOTING MACHINE ATTACKS

TUESDAY, SEPTEMBER 13, 2016

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Committee met, pursuant to call, at 10:11 a.m., in Room 2318, Rayburn House Office Building, Hon. Lamar Smith [Chairman of the Committee] presiding.

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6301
(202) 225-6371
www.science.house.gov

Protecting the 2016 Elections from Cyber and Voting Machine Attacks

Wednesday, September 14, 2016
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Witnesses

Dr. Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology

Hon. Tom Schedler, Secretary of State, State of Louisiana

Mr. David Becker, Executive Director, The Center for Election Innovation & Research

Dr. Dan S. Wallach, Professor, Department of Computer Science and Rice Scholar, Baker Institute for Public Policy, Rice University

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HEARING CHARTER

Tuesday, September 13, 2016

TO: Members, Committee on Science, Space, and Technology

FROM: Majority Staff, Committee on Science, Space, and Technology

SUBJECT: Full Committee hearing "Protecting the 2016 Elections from Cyber and Voting Machine Attacks"

The Committee on Science, Space, and Technology will hold a hearing titled *Protecting the 2016 Elections from Cyber and Voting Machine Attacks* on Tuesday, September 13, 2016, at 10:00 a.m. in Room 2318 of the Rayburn House Office Building.

Hearing Purpose:

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 EAC on technical, voluntary guidelines for voting. Since the voting process is regulated at the state level, the methods by which voter registration databases are managed and the ways that voters cast their ballots vary, and therefore, different guidance may be followed depending on the state.

The purpose of the hearing is to review the current voluntary guidelines for protecting voting and election systems, and whether such guidelines and protections are being effectively implemented in advance of the upcoming elections. This review will include the security of the election system in its entirety, including the security of: electronic voting machines, votes transmitted over the internet through email or e-fax, voter registration databases, and vote tally databases. In addition, the hearing will address the research and development that is underway to protect future voting and election systems.

Witness List

- **Dr. Charles H. Romine**, Director, Information Technology Laboratory, National Institute of Standards and Technology
- **Hon. Tom Schedler**, Secretary of State, State of Louisiana
- **Mr. David Becker**, Executive Director, The Center for Election Innovation & Research
- **Dr. Dan S. Wallach**, Professor, Department of Computer Science and Rice Scholar, Baker Institute for Public Policy, Rice University

Staff Contact

For questions related to the hearing, please contact Sarah Jorgenson or Raj Bharwani of the Majority Staff at 202-225-6371.

Chairman SMITH. The Committee on Science, Space, and Technology will come to order. Without objection, the Chair is authorized to declare recesses of the Committee at any time.

Welcome to today's hearing entitled "Protecting the 2016 Elections from Cyber and Voting Machine Attacks." I'll recognize myself for an opening statement and then the Ranking Member.

We are here today to discuss the subject of election security. It's hard to imagine a more bipartisan issue. Election security is fundamental to the fairness of elections and democracy in the United States. Elections are a key component of democracy, and voting is the very essence of what President Abraham Lincoln meant when he said a government by the people.

Voting is the means by which Americans express their opinions about their government. It provides Americans with the opportunity to affirm policies they like and change what they don't. When our citizens vote, they not only elect their leaders, they choose a direction and set priorities for our nation. Elections with integrity strengthen democracy. They confer legitimacy and boost public trust in government.

Concerns with earlier versions of voting and election systems led to the passage of the 2002 Help America Vote Act. This act requires the National Institute of Standards and Technology, over which we have jurisdiction, to work with the Election Assistance Commission on technical, voluntary guidelines for voting.

Today, we will discuss the current technical voluntary guidelines that are in place for States to protect their voting and election systems. Though these guidelines are voluntary, I hope to hear whether they are sufficient to safeguard our elections and whether States effectively use them.

This discussion is timely as many concerns have been raised in recent months about the vulnerabilities of electronic voting machines, voting over the Internet, and online voter registration. In response to these concerns, our discussion today will review the security of the election system in its entirety. We will examine what guidelines are in place, how we currently protect systems from potential technical vulnerabilities, and what kind of work—including research and development in my home State of Texas—is underway to protect future voting and election systems.

Last year, hackers from China infiltrated the Office of Personnel Management's database and stole confidential records and personal information on more than 22 million current and former federal employees, including those involved in our national security effort with the highest security clearances. The attacks on voter registration databases in Illinois and Arizona are the latest instances of such attacks, this time with alleged ties to Russia. We have yet to take decisive steps to defend ourselves and deter attackers.

The President says we are more technologically advanced, both offensively and defensively, in cyber warfare than our adversaries. So why won't he take the necessary steps to prevent cyber attacks on our elections systems by foreign governments? If we are attacked repeatedly and do nothing, we will have surrendered unilaterally and put at risk our economy, our national security, and our very freedoms.

This committee has held more than a half-a-dozen hearings on cybersecurity issues in this Congress. We know it isn't enough to respond to cyber attacks with diplomatic protest. We are going to hear from witnesses today about how the Federal Government can help States keep our election systems secure. But the single most important way to protect our election systems, to protect each American's right to vote and be heard, is for this Administration—and for the next Administration—to take decisive steps to deter and, if necessary, sanction foreign governments that attack us in cyber space.

[The prepared statement of Chairman Smith follows:]

COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
September 13, 2016

Media Contacts: Kristina Baum
(202) 225-6371

Statement of Chairman Lamar Smith (R-Texas)
Protecting the 2016 Elections from Cyber and Voting Machine Attacks

Chairman Smith: We are here today to discuss the subject of election security. It's hard to imagine a more bipartisan issue. Election security is fundamental to the fairness of elections and democracy in the United States.

Elections are a key component of democracy, and voting is the very essence of what President Abraham Lincoln meant when he said a government "*by the people*."

Voting is the means by which Americans express their opinions about their government. It provides Americans with the opportunity to affirm policies they like and change what they don't.

When our citizens vote, they not only elect their leaders, they choose a direction and set priorities for our nation.

Elections with integrity strengthen democracy. They confer legitimacy and boost public trust in government.

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 we have jurisdiction, to work with the Election Assistance Commission (EAC) on technical, voluntary guidelines for voting.

Today we will discuss the current technical voluntary guidelines that are in place that for states to protect their voting and election systems.

Though these guidelines are voluntary, I hope to hear whether they are sufficient to safeguard our elections and whether states effectively use them.

This discussion is timely as many concerns have been raised in recent months about the vulnerabilities of electronic voting machines, voting over the Internet, and online voter registration.

In response to these concerns, our discussion today will review the security of the election system in its entirety.

We will examine what guidelines are in place, how we currently protect systems from potential technical vulnerabilities, and what kind of work – including research and development in my home state of Texas – is underway to protect future voting and election systems.

Last year, hackers from China infiltrated the Office of Personnel Management's database and stole confidential records and personal information on more than 22 million current and former federal employees, including those involved in our national security effort with the highest security clearances.

The attacks on voter registration databases in Illinois and Arizona are the latest instances of such attacks, this time with alleged ties to Russia. We have yet to take decisive steps to defend ourselves and deter attackers.

The President says we are more technologically advanced, both offensively and defensively, in cyberwarfare arena than our adversaries. So why won't he take the necessary steps to prevent cyber-attacks on our elections systems by foreign governments?

If we are attacked repeatedly and do nothing, we will have surrendered unilaterally and put at risk our economy, our national security, our very freedoms.

This Committee has held more than a half a dozen hearings on cybersecurity issues in this Congress. We know it isn't enough to respond to cyber-attacks with diplomatic protests.

We are going to hear from witnesses today about how the federal government can help states keep our election systems secure. But the single most important way to protect our election systems, to protect each American's right to vote and be heard, is for this administration – and for the next administration – to take decisive steps to deter and, if necessary, sanction foreign governments that attack us in cyber-space.

###

Chairman SMITH. That concludes my opening statement, and the Ranking Member, the gentlewoman from Texas, Eddie Bernice Johnson, is recognized for hers.

Ms. JOHNSON. Thank you, Mr. Chairman, and good morning.

Ensuring that our elections are fair, accurate, and freely accessible to all American citizens is fundamental to our democracy. Every instance of malfunctioning voting technology and without question every cyber attack on our election system is significant. And all efforts to improve voting security, reliability, privacy, and access are welcome and important.

I am confident by the testimony of today's experts and many others that we are in a much better place today than we were 10 or 15 years ago. I'm deeply concerned, however, by some of the rhetoric in recent weeks that seems to—seems intended to erode public confidence in our election system. Prominent voices have suggested that the U.S. election system is riddled with fraud and somehow rigged. Those conspirator allegations, like many others, that have been floated in the public sphere this election cycle are not supported by actual facts, and they threaten the election process we have relied upon for more than 2 centuries.

I'm eager to hear from the distinguished panel today about the challenges of securing our election system in the digital age and what actions have been taken at the federal, state, and local levels to strengthen cybersecurity. However, given the reckless rhetoric, as well as other serious threats our election system is facing, I want to take this opportunity to put the cybersecurity challenges in context.

The U.S. election system is complex and highly decentralized, encompassing approximately 10,000 local, county, and state election offices. Further, there are few connections between individual voting systems and the Internet. And at least 75 percent of the voters will be able to verify their vote with a paper ballot this fall. This compartmentalization and paper trail provides a strong firewall against any cyber threats.

The recently publicized attacks against voter registration rolls in Arizona and Illinois are serious but have not resulted in any changes to voter data or to any voters. In Arizona the cybersecurity firewalls worked to contain the threat. What I find most concerning are reports that these recent threats may be linked to the Russian intelligence operation. So we must be vigilant, and I hope these incidents will lead to improved cybersecurity protocols and practices.

While security of the election system is important, voter access is fundamental to our democracy. Baseless allegations of widespread voter fraud have been used as an excuse to disenfranchise large numbers of minority and young voters through discriminatory voter ID restrictions.

News21, a journalism program established by the Carnegie Corporation of New York and the John S. and James L. Knight Foundation found voter impersonation fraud to be extraordinarily rare. An analysis of 2,068 alleged election fraud cases in all 50 States from 2000 to 2012 out of 146 million registered voters identified only 10 cases of voter impersonation fraud. You don't enact laws because of 10 cases of fraud in 12 years unless you have an ulterior

motive. Fortunately, the courts have been right through the most blatantly discriminatory state laws.

In addition to the state-sanctioned voter ID laws, the Brennan Center for Justice and others have continued to document cases of voter intimidation, deliberate spreading of misinformation to keep minorities and students from voting, and other attempts to target and disenfranchise minorities and young voters. These threats to tens of hundreds of thousands of eligible voters were either orchestrated by public officials or lone troublemakers should be taken as seriously as a cyber threat.

Mr. Chairman, I know my remarks have moved beyond the intended scope of this hearing, but you know well how passionate I am about this issue. It is my hope that with this hearing that we can have a thoughtful discussion of the challenges and actions that have been taken related to cybersecurity and other voting technology issues, while avoiding adding to the noise and confusion surrounding these issues just 8 weeks from the crucial election.

With that, I'd like to welcome our witnesses for being here today. And this is a distinguished panel. I look forward to hearing from our collective experience and expertise.

Thank you, Mr. Chairman. I yield back.

[The prepared statement of Ms. Johnson follows:]

OPENING STATEMENT
Ranking Member Eddie Bernice Johnson (D-TX)

House Committee on Science, Space, and Technology
"Protecting the 2016 Elections from Cyber and Voting Machine Attacks"
September 13, 2016

Thank you Mr. Chairman.

Ensuring that our elections are fair, accurate and freely accessible to ***all*** American citizens is fundamental to our democracy. Every instance of malfunctioning voting technology, and without question, every cyber-attack on our election system is significant. And all efforts to improve voting security, reliability, privacy, and access are welcome and important. I am comforted by the testimony of today's experts and many others that we are in a much better place today than we were 10 or 15 years ago.

I am deeply concerned, however, by some of the rhetoric in recent weeks that seems intended to erode public confidence in our election system. Prominent voices have suggested that the U.S. election system is riddled with fraud and somehow "rigged." Those conspiratorial allegations, like many others that have been floated in the public sphere this election cycle, are not supported by actual facts, and they threaten the election process we have relied upon for more than two centuries.

I am eager to hear from the distinguished panel today about the challenges of securing our elections system in the digital age, and what actions have been taken at the federal, state, and local levels to strengthen cybersecurity. However, given the reckless rhetoric as well as the other serious threats our elections system is facing, I want to take this opportunity to put the cybersecurity challenges in context.

The U.S. election system is complex and highly decentralized, encompassing approximately 10,000 local, county, and state election offices. Further, there are few connections between individual voting systems and the Internet, and at least 75 percent of voters will be able to verify their vote with a paper ballot this Fall. This compartmentalization and paper trail provides a strong firewall against any cyber threats.

The recently publicized attacks against voter registration rolls in Arizona and Illinois are serious, but have not resulted in any changes to voter data or to any votes. In Arizona, the cybersecurity firewalls worked to contain the threat. What I find most concerning are reports that these recent threats may be linked to Russian intelligence operations. So we must be vigilant, and I hope these incidents will lead to improved cybersecurity protocols and practices.

While security of the election system is important, voter **access** is fundamental to our democracy. Baseless allegations of widespread voter fraud have been used as an excuse to disenfranchise large numbers of minority and young voters through discriminatory voter ID restrictions. News21, a journalism program established by the Carnegie Corporation of New York and the John S. and James L. Knight Foundation, found voter impersonation fraud to be extraordinarily rare. An analysis of 2,068 alleged election-fraud cases in all 50 states from 2000 to 2012 out of 146 million registered voters identified only 10 cases of voter impersonation fraud. You don't enact laws because of 10 cases of fraud in 12 years unless you have an ulterior motive. Fortunately, the courts have seen right through the most blatantly discriminatory state laws.

In addition to the state-sanctioned voter ID laws, the Brennan Center for Justice and others have continued to document cases of voter intimidation, deliberate spreading of misinformation to keep minorities and students from voting, and other attempts to target and disenfranchise minority and young voters. These threats to tens or hundreds of thousands of eligible voters, whether orchestrated by public officials or lone trouble-makers, should be taken just as seriously as the cyber threat.

Mr. Chairman, I know my remarks have moved beyond the intended scope of this hearing. But you know well how passionate I am about this issue. It is my hope with this hearing that we can have a thoughtful discussion of the challenges and actions that have been taken related to cybersecurity and other voting technology issues, while avoiding adding to the noise and confusion surrounding these issues just 8 weeks out from a crucial election.

With that, I would like to welcome all of our witness for being here today. This is a distinguished panel, and I look forward to learning from your collective experience and expertise.

Thank you Mr. Chairman. I yield back.

Chairman SMITH. Okay. Thank you, Ms. Johnson. And I'll introduce our witnesses. Our first witness today is Dr. Charles Romine, Director of the Information Technology Laboratory at the National Institute of Standards and Technology. In this capacity, Dr. Romine oversees a research program that develops and disseminates standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, which includes cybersecurity standards and guidelines for federal agencies in U.S. industry.

Dr. Romine previously served as a Senior Policy Analyst at the White House Office of Science and Technology Policy and is a Program Manager at the Department of Energy's Advanced Scientific Computing Research Office.

Dr. Romine received both his bachelor's degree in mathematics and his Ph.D. in applied mathematics from the University of Virginia.

I'll now recognize the gentleman from Louisiana, Mr. Abraham, to introduce our next witness, who happens to also be from Louisiana.

Mr. ABRAHAM. Thank you, Mr. Chairman. It is my pleasure to recognize Hon. Tom Schedler, the Secretary of State from the great State of Louisiana. Secretary Schedler was appointed to the position in 2010 and was reelected in 2011 to serve a four-year term. He is past President of the National Association of Secretaries of State with his term ending this past July. And he served as Co-Chairman for the National Association of Secretaries of State Task Force on Emergency Preparedness for Elections.

As Secretary of State of Louisiana, he is committed to protecting and defending the integrity of every election in the State and has worked diligently to streamline the election process. The result is been a more efficient and cost-effective system with Louisiana becoming one of the first States to implement online voter registration and the first State in the country to launch a smartphone app for voters to use to get timely election information. My pleasure for you to be here.

I yield back, Mr. Chairman.

Chairman SMITH. Thank you, Mr. Abraham.

Our third witness today is Mr. David Becker, Executive Director and Co-Founder of the Center for Election Innovation and Research. Mr. Becker founded CEIR to increase voter turnout and give election officials the tools they need to ensure all eligible voters can vote conveniently and assist them with maximum integrity.

Prior to founding CEIR, Mr. Becker was the Director of the Elections Program at the Pew Charitable Trust where he worked on reforms in election administration. These reforms included using technology to provide voters with information they need to cast a ballot.

Mr. Becker received both his undergraduate and law degrees from the University of California at Berkeley.

Our final witness today from my home State of Texas is Dr. Dan Wallach, Professor in the Department of Computer Science and Rice Scholar at the Baker Institute for Public Policy at Rice University. Dr. Wallach's research covers a variety of topics in computer security. This includes electronic voting system security

where he served as the Director of an NSF-funded multi-institution research center, A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections, acronym for which is ACCURATE. He also served as a member of the Air Force Science Advisory Board from 2011 to 2015.

Dr. Wallach earned his bachelor's degree in electrical engineering and computer sciences at UC Berkeley and his master's and Ph.D. from Princeton University.

We welcome you all, appreciate your expert advice.

And, Dr. Romine, if you'll begin.

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

Dr. ROMINE. Thank you, Mr. Chairman. Chairman Smith, Ranking Member Johnson, and Members of the Committee, thank you for the opportunity to discuss NIST's role in voting systems.

Improving voting systems requires an interdisciplinary, collaborative approach that must be accurate and reliable, yet cost-effective, secure, and usable and accessible to all voters. The design and standards must consider the diversity of voting processes and ballots across the States, and none of these can be considered in a vacuum.

NIST expertise in testing, certification, information security, trusted networks, software quality, and usability and accessibility provides the foundation for our voting systems work, but our experience working in multi-stakeholder processes is critical. We must bring together election officials, industry, technical experts, and advocacy groups to address this challenge.

The NIST role is limited to the research to develop standards, tests, guidelines, best practices, and assistance with laboratory accreditation that the Election Assistance Commission, or EAC, and state and local jurisdictions may use at their discretion.

Since the signing of the Help America Vote Act, or HAVA, NIST has partnered with the EAC to develop the science, tools, and standards necessary to improve the accuracy, reliability, usability, accessibility, and security of voting systems. Our joint accomplishments include new voting system guidelines; guidelines in support of Military and Overseas Voters Empowerment Act, or MOVE; and the Uniformed and Overseas Citizens Absentee Voting Act, or UOCAVA; the establishment of accredited testing laboratories for voting system equipment and a testing and certification program upon which many States depend.

The Technical Guidelines Development Committee, or TGDC, a federal advisory committee to the EAC chaired by NIST, assists in the development of the voluntary voting system guidelines. In 2015, the EAC approved the TGDC's latest recommendations, Voluntary Voting System Guidance, or VVSG 1.1, with new requirements for human factors, audit and election logging, and new security requirements on access control, physical security, auditing, cryptography, software quality, and software integrity.

To support overseas and military voters, including the use of the Internet to cast absentee ballots, NIST research concluded that widely deployed security technologies and procedures could miti-

gate many of the risks associated with electronic blank ballot delivery but the risks associated with casting doubts over the Internet were more serious and challenging to overcome.

Based on that research, NIST documented security best practices and considerations for election officials on the use of electronic mail or the Web to expedite transmission of voter registration materials and blank ballots. In early 2011, NIST analyzed current and emerging technologies that may mitigate risk to Internet voting.

We also identified several areas where research and technological improvements are needed to ensure the security, usability, and accessibility of Internet voting. Many of these challenges are not unique to Internet voting such as strong identity management, protection against malware, and the resiliency of Internet-connected systems. The unique challenges of Internet voting are the requirements and expectations, notably ensuring the integrity of the voting process while protecting privacy.

NIST and the EAC have recently organized public working groups that provide an open and transparent development process and give the EAC and state election officials the opportunity to work directly with academic, industry, and Federal Government experts. The working groups help inform NIST, the EAC, and the TGDC in updating the VVSG.

There are three election working groups—pre-election, election, and postelection—that are providing insight on election processes. These groups are supported by four technical groups—cybersecurity, human factors, interoperability, and testing. The election working groups take input from the technical groups to inform requirements development for consideration by the TGDC.

Ensuring that voting systems are secure and auditable is critical to providing trust and confidence in the voting process. The cybersecurity technical working group is developing guidelines and best practices to secure voting systems. The group is focused on election security best practices, including physical security, auditing, and contingency planning.

To provide a firm foundation for next-generation security guidelines, NIST is researching threats and vulnerabilities to voting systems and the best practices and technologies that can mitigate those risks. As part of that research, NIST has catalogued published vulnerabilities and weaknesses in voting system software. The goal is to understand the types of vulnerabilities by looking at historical evidence and creating a voter-specific list of vulnerabilities and mapping these with weaknesses to requirements in the VVSG. This work has identified issues that should be addressed in future security requirements and test methods and by voting system manufacturers.

NIST is committed to continue collaborating with the EAC and others to fulfill our role defined in HAVA, MOVE, and UOCAVA. We leverage our research, which is applicable to a wide variety of organizations and used by industry and governments throughout the world. Active collaboration between the public and private sectors is the only way to effectively meet this challenge, leveraging each participant's roles and responsibilities.

Thank you for the opportunity to testify today on NIST's work in voting systems, and I would be happy to answer any questions 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

Protecting the 2016 Elections from Cyber and Voting Machine Attacks

September 13, 2016

INTRODUCTION

Chairman Smith, Ranking Member Johnson, and members of the Committee, I am Dr. 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 key role in voting systems.

THE ROLE OF NIST IN VOTING SYSTEMS

With programs focused on national priorities from the Smart Grid and electronic health records to forensics, atomic clocks, advanced nanomaterials, computer chips and more, NIST's overall 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. NIST's role in voting draws on our expertise in providing measurements, working with standards development organizations, and the development of testing and certification infrastructures necessary to support standards implementation.

Improving voting systems requires an interdisciplinary, collaborative approach. They must be accurate and reliable, yet cost-effective. They must be secure and usable. And, of course, they 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 and certification, information security, trusted networks, software quality, and usability and accessibility provides the technical foundation for our voting systems work, but our experience working in multi-stakeholder processes is also critical to this effort. We must bring together election officials, industry, technical experts, and advocacy groups to address this challenge. However, the NIST role is limited to the research to develop standards, tests, guidelines, best practices and assistance with laboratory accreditation that the Election Assistance Commission[1] (EAC), and state and local jurisdictions may use at their discretion. Further, neither the EAC nor NIST are empowered to regulate state and local electoral systems, and as NIST is a non-regulatory agency none of the guidelines and best practices offered by NIST are mandatory.

Historical Perspective

In 1974, the National Bureau of Standards (now the National Institute of Standards and Technology) began a research project funded by the Office of Federal Elections of the General Accounting Office. This project resulted in a 1975 report, later reprinted as NIST Special Publication (SP) 500-30, Effective Use of Computing Technology in Vote-Tallying. The report provided findings and conclusions about improving the accuracy and security of the vote-tallying process, improving the management of the election preparation process, and institutional factors affecting accuracy and security. The report also pointed out the lack of systematic research on election equipment and systems, and on human engineering of voting equipment, and it concluded that the setting of national minimum standards for federal election procedures would serve a valuable function.

[1] http://www.eac.gov/default.aspx.

Legislative Mandates

Since the signing of the Help America Vote Act of 2002[2] (HAVA) and reinforced by the Military and Overseas Voter Empowerment Act[3] (MOVE), the NIST Voting Program has partnered with 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.

HAVA assigned three major items to NIST. First, NIST was assigned the development of a report to assess the areas of human factors research, which could be applied to voting products and systems design to ensure the usability and accuracy of voting products and systems. Second, NIST was tasked with chairing and providing technical support to the Technical Guidelines Development Committee (TGDC), Federal Advisory Committee to the EAC, in areas including (a) the security of computers, computer networks, and computer data storage used in voting systems, (b) methods to detect and prevent fraud, (c) the protection of voter privacy, and (d) the role of human factors in the design and application of voting systems, including assistive technologies for individuals with disabilities and varying levels of literacy. Third, NIST was to conduct an evaluation of independent, non-Federal laboratories and to submit to the EAC a list of those laboratories that NIST proposes to be accredited to carry out the testing.

The TGDC, first met in July 2004 to assist the EAC in the development of the voluntary voting system guidelines and established three subcommittees, focused on security and transparency; human factors and privacy; and core requirements and testing. The TGDC delivered its initial set of recommendations to the EAC in April 2005. Those recommendations, *Voluntary Voting System Guidance* (VVSG) 1.0, augmented the 2002 Voting System Standards by including security measures for auditability, wireless communications and software distribution and set up, and improvements for the accessibility guidelines and usability design guidelines for voting systems.

ACCOMPLISHMENTS

The NIST/EAC partnership is well over a decade old. Our joint accomplishments include:

- new voting system guidelines
- guidelines in support of MOVE and the Uniformed and Overseas Citizens Absentee Voting Act[4] (UOCAVA)
- the establishment of accredited testing laboratories for voting system equipment; and
- a testing and certification program upon which many states depend either in whole or in part.

VVSG: 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. The VVSG also address physical and systems level security. The Guidelines are used by accredited testing laboratories as part of both

---

[2] Pub. L. No. 107-252, (Oct. 29, 2002) 116 Stat. 1666, codified in relevant part at 52 U.S.C. 20901 et seq.
[3] Pub. L. No. 111-84, div. A, title V, (Oct. 28, 2009) 123 Stat. 2319, codified in relevant part at 52 U.S.C. § 20311.
[4] Pub.L.No. 99-410, title I, § 102, (Aug. 28, 1986), 100 Stat. 925.

state and national certification processes, 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.

VVSG 1.0 also provided a set of specifications and requirements against which voting systems can be tested to determine if they possess the requisite functionality, accessibility and security capabilities. In addition, the guidelines established evaluation criteria for the national certification of voting systems. The VVSG and the related testing efforts, although voluntary for states, are in use in whole or in part by 47 out of 50 states. Work began on a new set of guidelines after the adoption of the VVSG 1.0. A draft of these guidelines was released for public comment in 2007 and, after much debate, many of the proposed guidelines were included the VVSG 1.1 This addressed new requirements for human factors, audit and election logging, quality assurance and configuration management, as well as new security requirements on access control, physical security, auditing, cryptography, software quality, and software integrity. In January 2015, the newly appointed EAC approved the latest version, deemed VVSG 1.1, or VVSG 2015.

UOCAVA: To support the Federal Voting Assistance Program's (FVAP) mission to help overseas and military voters exercise their right to vote, NIST has conducted research on the use of electronic technologies in the absentee voting process, including casting ballots over the Internet. To identify the potential risks, NIST produced NISTIR 7551, A Threat Analysis on UOCAVA Voting Systems, which analyzed the use of several electronic technologies for different aspects of the absentee voting process. This research concluded that widely-deployed security technologies and procedures could mitigate many of the risks associated with electronic blank ballot delivery, but that the risks associated with casting ballots over the Internet were more serious and challenging to overcome. Based on that research, NIST developed two additional documents covering security best practices for UOCAVA voting, NISTIR 7711, Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters and NISTIR 7682, Information System Security Best Practices for UOCAVA-Supporting Systems. These two documents serve as companion documents to one another. NISTIR 7711 provides security best practices and considerations for election officials on the use of electronic mail or Web sites to expedite transmission of voter registration materials and blank ballots. NISTIR 7682 provides best practices for those configuring and administering IT systems used to support UOCAVA voting. In early 2011, NIST released NISTIR 7770, Security Considerations for Remote Electronic UOCAVA Voting which studied Internet voting in more detail. This report identified and analyzed current and emerging technologies that may mitigate risks to Internet voting. It also identified several areas where additional research and technological improvements are needed to ensure the security, usability and accessibility of Internet voting. Many of these challenges are not unique to Internet voting, such as strong identity management, protection against malware, and the resiliency of Internet-connected systems. The unique challenges of Internet voting are the requirements and expectations – notably, ensuring the integrity of the voting process while also protecting voters' privacy.

Accredited Laboratories and Testing and Certification Program: Section 231 of HAVA requires EAC and NIST to develop a national program for accrediting Voting System Test Laboratories (VSTL) to conduct testing of voting systems and components, providing a measure of confidence that such laboratories are capable of performing testing to meet the requirements. A laboratory

achieving National Voluntary Laboratory Accreditation Program (NVLAP) accreditation is recommended by NIST to the EAC for designation as EAC-accredited VSTL. The EAC maintains a list of accredited VSTLs to help vendors and elections officials identify resources to fulfill system testing requirements. EAC-accredited VSTLs test voting systems for conformance with the voluntary voting system standards. Laboratory test reports are reviewed by the EAC for compliance with certification requirements. At this time, 47 states either require national certification or utilize the national standards when certifying voting systems.

In addition to national certification, state certification tests are performed to confirm that the voting system presented is the same as the one certified under the Guidelines.

- Acceptance tests are performed at the state or local jurisdiction level upon system delivery by the manufacturer to confirm that the system delivered is the specific system certified by the EAC and, when applicable, certified by the state.
- Election personnel conduct voting equipment and voting system readiness tests prior to the start of an election to ensure that the voting system functions properly, to confirm that voting equipment has been properly integrated, and to obtain equipment status reports.
- Election officials also perform verification at the polling place and any central locations used for vote counting to ensure that all voting systems and voting equipment function properly before, during, and after an election.

NIST works actively with the election community to support the development of tests used by the VSTLs for certification. Test assertions are measurable expressions that must be tested to evaluate conformance of an implementation (in this case a voting system) to a requirement. The goal of creating these test assertions is to make clear to testing laboratories and manufacturers of voting systems the specific conditions of each VVSG requirement that must tested to be certified by the EAC. Different testing laboratories, using this set of test assertions, should arrive at the same pass/fail results for each requirement in the VVSG, thus helping to ensure uniformity in testing among testing laboratories. These test assertions were developed by NIST and distributed to EAC and testing laboratories for their comments. For VVSG 1.0, NIST developed and updated, based on public comments, 1138 test assertions covering usability, accessibility and security requirements. For VVSG 1.1, there are an additional 597 test assertions, covering security and quality and configuration management in the review process.

RECENT ACTIVITIES

The VVSG development has been focused on developing guidelines for voting systems that are used on election day, for casting and counting ballots. After voters are checked in, they mark their ballots using one of three methods – electronic machines, ballot marking devices that produce a paper ballot, or directly on paper. New technologies are entering the marketplace, including those that support online voter registration systems, electronic pollbooks (e-pollbooks), electronic ballot marking, ballot on demand, ballot delivery, election reporting and auditing. These systems replace paper-based equivalents with electronic methods, with an increased use of tablets and connected or online options.

There is much debate over whether these election systems should be addressed in the VVSG and thus require federal testing and certification. It is clear that additional guidance is necessary to secure increasingly connected or online systems. The move towards tablets provides superior

usability and accessibility features, but requires new guidelines to allow all voters to vote independently and privately using these new devices, new interfaces, and new modes of interaction. Interconnected systems must also be able to communicate among components using standard protocols.

Open and Transparent Process

In February 2015, NIST and the EAC cosponsored the second of two symposiums aimed at ensuring that the technology and standards for voting systems support verifiable, fair elections, an essential element of our U.S. democracy. The first symposium, in February 2013, brought together election officials, voting system manufacturers, test labs, standards developers, researchers, and advocates to discuss standards and conformance testing processes that are needed to best accommodate future voting systems and the needs of election officials and voters. The theme of the second Symposium was "The People, The Process, The Technology". The purpose was to ensure we are responding appropriately to the many recent changes in voting technology and are prepared to respond to future updates. More than 540 government, industry, and academic representatives attended the workshop, and/or participated via live webcast.

NIST and the EAC organized public working groups that provide an open and transparent development process and gives the EAC and state election officials the opportunity to work directly with academic, industry, and federal government experts. The working groups help inform NIST, the EAC and the TGDC in creating a new version of the VVSG. The creation of the working groups was done as a direct response to feedback received from the Presidential Commission on Election Administration[5], EAC Standards Board as well as from the National Association of State Election Directors[6]. Each of these groups expressed interest in being involved in the process throughout the development, rather than only after the draft standard is released for public comment. This new process allows the working groups to take advantage of the expertise of the many election officials and other subject matter experts across the country who are willing to volunteer their time and offer their input.

There are three election working groups (pre-election, election and post-election) that are providing insight on election processes via the development of models and assessing the impact of integrating electronic equivalents into their processes. These groups are supported by four technical groups covering cybersecurity; human factors, including accessibility and usability; interoperability; and testing. The election working groups take input from the technical groups to inform requirements development for consideration by the TGDC. There are currently more than 400 members across the seven public working groups.

Our common goal, of course, is to ensure that the next generation of technology and standards for voting systems support verifiable, fair elections. Through the election working groups, we've already made progress in:

- creating a detailed understanding of elections through the creation of process models,
- identifying what well-established procedures are already in place, and
- documenting how technology is playing an increasing role in the election processes.

[5] https://www.supportthevoter.gov/
[6] https://www.nased.org/

Using the election models as input, the TGDC has discussed the increased use of digital systems and has identified several areas for additional investigation. These areas include: voter registration databases, e-pollbooks, ballot delivery, ballot on demand, ballot marking, election-night reporting, and auditing. NIST developed a set of use cases that further explored possible scenarios within these areas. The technical working groups are now reviewing the VVSG with a focus on these use cases, performing a gap analysis, and providing work plans for the development of new guidelines.

NIST has designed a new approach to developing standards for emerging voting system technologies based on a structure of high level principles and guidelines that is more responsive to rapidly changing technology and the needs of election officials. This structure is useful in identifying gaps in the existing requirements and also provides a design for the next generation VVSG document that will provide a more intuitive way for election officials as well as advocates, developers, and test labs to find, understand, and navigate the guidelines, requirements, and test assertions.

Usability and Accessibility

In 2015, NIST funded development of a roadmap for improving the usability and accessibility of next generation elections, with input from a cross-section of election officials, advocacy groups, academics, and the EAC. Following this roadmap, the human factors technical working group is addressing accessibility and usability issues and requirements that pertain to where voters, poll workers, and election officials interact with the electronic voting system at the polling place. The working group developed a set of five human factors voting principles with supporting guidelines and are using these to guide the their discussions about requirements for new voting system technologies. This structure has proven particularly useful in identifying gaps in the existing usability and accessibility requirements.

NIST also has worked with the election community to develop draft guidance in two other areas: (1) a protocol for testing the usability of e-pollbooks and a checklist for ease-of-use considerations that election officials can turn to when acquiring e-pollbooks and (2) usability, accessibility and security guidance for remote ballot marking to enable voters with disabilities to mark their ballots independently at home using their own assistive technology that can then be mailed or delivered to the polling place for casting.

Interoperability

The goal of the interoperability technical working group is to enable voting systems to become interoperable and thus assist election officials in having more choice in the market. A critical element to voting system interoperability, the Common Data Format (CDF) for election data, was initiated within the IEEE and is now being developed within the interoperability technical working group. Its first output, NIST SP 1500-100, constitutes an interoperable CDF for the election data commonly processed by election management systems, which includes election setup data (e.g., contest/candidate info, ballot preparation, political geography configuration) and election results data. This CDF was used by Ohio and the Associated Press for publishing and receiving its 2014 and 2016 primary and general election results and adopted by Google and Pew Research for use in their voting information projects; several other States and manufacturers have expressed their desire to use and support this format in products. The next CDF Specification, Draft NIST SP 1500-101 Election Log Export, addresses election system logging

and auditing and is being readied for publication. The group is working currently on three other CDF specifications:

- Voter Registration Data: for registration-related data imported and exported from voter registration systems and other sources such as the DMV.
- Cast Vote Records: for voted ballot data exported from voting devices and used for tabulation and election audits.
- E-Pollbooks: for data used in check-in at the polls and updates to voter records.

Cybersecurity

Ensuring that voting systems are secure and auditable is critical to providing trust and confidence in the voting process. To provide a firm foundation for next-generation security guidelines, NIST staff are researching threats and vulnerabilities to voting systems, and the security best practices and technologies that can mitigate those risks.

Software Vulnerabilities and Weaknesses: As part of that research, NIST has cataloged published vulnerabilities and weaknesses in voting system software using the Common Weakness Enumeration (CWE). The overarching goal of the work is to understand the types of vulnerabilities in voting systems by looking at historical evidence and creating a voting-specific list of vulnerabilities. CWE provides a common language for describing software security weaknesses in architecture, design, or code and is used worldwide in industry, government, and academia as a common method to communicate software vulnerabilities. Use of the CWE definitions can provide a common baseline for weakness identification, mitigation, and prevention efforts and can serve as a measurement for software security tools targeting those weaknesses. This research has identified over 250 weaknesses in the areas of authentication, cryptography, input validation, and privilege management. Further, NIST mapped these weaknesses to software security requirements in the VVSG 1.0 and VVSG 1.1. This work will provide valuable input to the VVSG development process, and has identified issues that should be addressed in future security requirements and test methods and by voting system manufacturers.

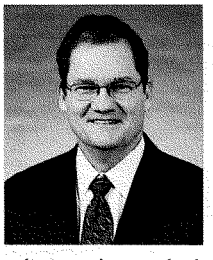
The *cybersecurity technical working group* is developing guidelines and best practices to secure voting systems, with the primary objective of contributing to the development of the next VVSG. The work of this group is intended to inform the decisions and activities of the TGDC and the election working groups. The group is currently focused on election security best practices, including physical security, auditing, and contingency planning. These discussions will inform future activities by NIST and the EAC. To support the development of the next version of the VVSG, the group is identifying security principles that will drive the development of new security requirements and test assertions. These principles are being derived from past versions of the VVSG, augmented by other cybersecurity guidelines and working group discussions. In the near-term, the group will also investigate a number of election use cases that were identified as priorities by NIST and the EAC working in collaboration with election officials. The group will consider security issues associated with each use case and identify gaps in the existing guidelines. This information will be used to scope and prioritize the next VVSG.

CONCLUSION

NIST is committed to continue collaborating with the EAC, the FVAP, election officials and others to fulfill our role defined in HAVA, MOVE and UOCAVA. We leverage our work in the areas of testing and certification, information security, trusted networks, usability, and software quality, which are applicable to a wide variety of organizations, and are used by industry and governments throughout the world. Active collaboration within the public sector, and between the public and private sectors, is the only way to effectively meet this challenge, leveraging each participant's roles, responsibilities, and capabilities.

Thank you for the opportunity to testify today on NIST's work in voting systems. I would be happy to answer any questions you may have.

Charles H. Romine, Ph.D.



Charles Romine is Director of the Information Technology Laboratory (ITL). ITL is one of seven research Laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of $150 million, more than 440 employees, and about 150 guest researchers from industry, universities, and foreign laboratories.

Dr. Romine oversees a research program designed to promote U.S. innovation and industrial competitiveness 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.

Chairman SMITH. Thank you, Dr. Romine. And, Secretary Schedler.

TESTIMONY OF HON. TOM SCHEDLER, SECRETARY OF STATE, STATE OF LOUISIANA

Mr. SCHEDLER. Thank you. I want to thank the Committee, Chairman Smith, and Ranking Member Johnson for the invitation to address you today. I think it's very important for you to hear from actual election officials who actually conduct elections. And our job—at least in my opinion, is to make voting easier, more accessible, and to make it tough to cheat.

But in recent weeks, reports on cyber attacks have voters questioning whether their vote will actually count, and that in my opinion is more damaging than the potential for hacking.

We are all on high alert. This whole exercise has put every one of the 50 States working on national security issues with all national agencies in an effort to try to improve the system we have or to recheck the system we have. But the fact is States are always evaluating security measures and emergency plans. As I speak, in Louisiana I'm dealing with 30 precincts from the record flooding that we had in the Baton Rouge area on contingency plans and what I'm going to do to move those precincts, notify voters, and the like.

So yes, we—are we concerned about potential interference into our election process? We absolutely are, but voter fraud is much, much harder to accomplish than you may think. As was pointed out by Ranking Member Johnson, we have some 10,000 jurisdictions of voting in this country hundreds of thousands of voting machines in various locations. The complexity of our election system has reinforced the election process, and what I mean by that is if you think about the complexity of that, it makes it very difficult for any player to go in and actually disrupt a federal national election.

Specifically, States have developed online registration some 31 States have the best practice to improve customer service. They've also developed different ways to guard against intrusion. In Louisiana, for instance, information collected through our online voter registration system does not flow directly into our statewide system. Instead of voter information is sent from a Web site to each parish register in the State of Louisiana. The register has direct access to the database, not the voter.

While it would certainly be disruptive to have registration systems hacked, as we saw in Arizona and Illinois, voters could still vote and Election Day would still occur. Anyone who discovers an issue with their voter registration status still has the option of a provisional ballot. And remember, no voter information was added or deleted in Arizona or Illinois, and most States have electronic paper ballot backups.

In terms of voting machines, it's important to note that so far scientists have only succeeded in hacking voting machines when favorable conditions existed that do not exist on Election Day, including plenty of time and unfettered access. There is no evidence that ballot manipulation has ever occurred in the United States.

No State—and I want to make this clear—has Internet voting, and our voting machines are never connected to the Internet. In Louisiana, all machines are stored in secure, state-owned warehouses. All maintenance, including most up-to-date software applications, as well as programming, is performed by vetted Secretary of State employees, not outside contractors.

Additionally, before every election, Louisiana publicly performs a test-and-seal process in which we demonstrate that each machine is working properly before it is locked with a tamperproof seal. That testing process is also done at the end of each Election Day to demonstrate that each machine is functioning postelection, which is required by roughly 60 percent of the States. And, if necessary, the majority of States can make paper ballots and audits available if a recount or review becomes necessary.

Finally, please keep in mind that timing is critical. Elections are no longer one-day events and voting is occurring right now as we speak. Ballots have been printed, absentee ballots are in the mail, and in-person voting begins in days in some States. To say this is an inopportune time for election officials to be discussing this subject instead of real-time preparation is an understatement. The train has left the station.

During a call with Secretary Jeh Johnson in mid-August, my colleagues and I were assured there would be no intent to declare an election system as part of the critical infrastructure before the November elections. Some Secretaries, including myself, have been very vocal that no matter when that may occur, such a designation would undercut the Constitutional role of the States and local jurisdictions. It would only complicate our ability to properly secure elections.

As of today, there is not enough clear information on what the designation would mean or why it's necessary. States get what we need through existing networks, including the United States Elections Assistance Commission and the National Institute of Standards and Technology, which already identify the kind of testing and certification.

And most standards needed to reveal signs of tampering, there is a role for Congress in this. Most States purchase their voting machines using federal dollars, HAVA, back in 2005, but there is little interest on the Hill when it comes to helping replace our aging systems. I suggest you revisit HAVA and see how an investment in voting technology could benefit our nation in the long run.

In the meantime, we have received a sobering wake-up call on the serious nature of cyber attacks. States will continue to take a proactive approach to secure our election systems, and at the end of the day, I want to assure every American—and I speak for all of my colleagues, the Secretaries of State Association—that your next President will be determined by the vote of the people and every vote will count.

Thank you for allowing me my comments.

[The prepared statement of Mr. Schedler follows:]

Testimony on Election Security by the Hon. Tom Schedler, Louisiana Secretary of State

Thank you. I'm here today to talk about the security of the elections process from my perspective as Louisiana Secretary of State and past president of the National Association of Secretaries of State, which represents a majority of the nation's chief state election officials.

First, let me thank the Committee and Chairman Smith for the invitation to participate. It's important for you to hear directly from the authorities who oversee elections in this country. Our job is to make voting easy and cheating hard.

In light of recent events, including reports that parties tied to Russia may be behind recent efforts to mine data from voter registration systems in at least two states, the message is clear: We are now on high alert against foreign cyber threats that may be trying to impact our elections. States and localities must remain vigilant and take every necessary precaution to secure our election and voting systems against credible threats.

We are committed to working with national security agencies and regular federal partners to solicit input on cyber threat response and risk mitigation in our elections. States are already deploying numerous resources for this cycle, including extensive testing for cyber threats described in a recent FBI alert. Additional steps may be taken based upon credible or specific threats that are identified in the run-up to Election Day. Secretaries of State are also taking part in a Department of Homeland Security Election Infrastructure Cybersecurity Working Group, created for sharing resources, best practices and technical advice.

The risks posed by foreign government hackers, cyber criminals and everyday hacktivists are not a new concept for election officials. In fact, states are *always* evaluating and adapting security measures to protect the integrity of our elections as part of emergency preparedness planning. As we speak, local officials in Louisiana are moving approximately thirty precincts in the wake of the historic flooding that inundated the Baton Rouge area in August.

Just as we must have contingency plans for floods and all kinds of natural phenomena, we must also be ready to deal with man-made threats. As we collaborate on appropriate steps to be taken, there are several key points that I want to share with you.

Our System Has Built-In Safeguards Against Systemic Fraud

For starters, we must ensure that actions to protect our elections do not create UNDUE alarm that can threaten voters' confidence in election outcomes, or end up perceived as a federal power grab over the voting process.

Our system has built-in safeguards against systemic fraud. Elections are administered by states and localities, with a minimal amount of federal involvement. Voting systems are spread out in a highly-decentralized structure covering more than 9,000 election jurisdictions and hundreds of thousands of polling locations. Voting machines are standalone and not designed to connect to the Internet. There are multiple layers of physical and technical security surrounding our systems.

While no state wants to see its voter registration system breached, the targeting of such systems does not easily result in fraud or disenfranchisement. This is because non-voting components of the election process have their own fail-safes and contingency solutions that make it extremely difficult to leverage them for changing election outcomes. In fact, no voter information was found to be added or deleted in recent state voter registration system breaches.

In Louisiana, information collected through our online voter registration system does not flow directly into our statewide registration database. Instead, voter information is sent from the website to each parish (county) registrar of voters' office for verification and final processing. Poll books, printed records, back-ups, and back-ups of back-ups also provide multiple layers of security around this part of the process.

Plus, anyone who discovers an issue with their voter registration status when they show up at a polling place still has options for casting a ballot.

Identifying and Understanding Legitimate Cyber Threats

Now to the voting machines. I'm happy to report that there is no evidence that ballot manipulation has ever occurred in the U.S. as the result of a cyberattack. As I've already stated, voting systems are standalone and do not connect to the Internet. The nationwide trend has been toward the adoption of voting systems that create both paper and electronic records, a combination that makes detection easy.

Before every election, Louisiana publicly performs a "test and seal" process in which we demonstrate that each machine is working properly before it is locked with a tamper-proof seal that is not removed until election morning. This testing process is repeated at the end of each election to again demonstrate that each machine is functioning as it was designed. State laws typically require voting equipment to be physically secured when not in use.

In all states, tabulations aren't final until the completion of an official canvass to review vote counting and certify the results. Election night reporting (ENR) systems may utilize electronic transmissions of tabulated voting results for reporting purposes, but they are always unofficial numbers subject to review. In Louisiana, just like our registration database, the public website is not where results are accumulated or tallied. The unofficial results are sent to Baton Rouge from across the state on closed lines using computers that are used only for election night transmissions. They are never connected to the internet. Those results are then processed and saved before they are shared on the public site. In other words, the public site has a secure backup that includes several layers of security.

Post-election audits, which are required in roughly sixty percent of all states, can help to further safeguard against deliberate manipulation of the election, as well as unintentional software, hardware or programming problems. If necessary, the majority of states can make paper ballots and/or audits available for recount or review.

Timing is Critical to this Conversation

Finally, please keep in mind that timing is critical right now. Elections are no longer one-day events. Ballots are printed, absentee ballots are in the mail and in-person early voting is nearly ready to begin. absentee ballots are in the mail and in-person voting begins in days in some states. To say this is an inopportune time for elections officials to be discussing this

topic instead of real time preparations would be an understatement. During a call with DHS Secretary Jeh Johnson in mid-August, my colleagues and I were assured that the Department of Homeland Security has no intention of declaring our election system to be part of the nation's "critical infrastructure" before the November presidential election.

Many Secretaries of State, including myself, have been very vocal in their belief that no matter when it might occur, such a designation would greatly undercut traditional state and local control of elections and serve as a major distraction in moving forward together in securing our elections.

As of today, there isn't enough clear information on what this designation would mean, or why it is necessary, given that states can get what they need through existing federal networks. For example, the U.S. Election Assistance Commission and NIST (National Institute of Standards and Technology) can provide ongoing assistance to states by identifying the kind of testing that would reveal signs of tampering that a sophisticated nation-state adversary might conduct.

There is a role for Congress as well. Most states purchased their voting machines using federal dollars supplied by the Help America Vote Act (HAVA) back in 2005, but there is little interest from the Hill when it comes to helping officials replace these aging systems. In 2010, NASS produced a funding report noting that $396 million in HAVA funding remains to be appropriated. I suggest you revisit HAVA and see how an investment in voting technology could benefit our nation for the long-term.

In the meantime, we have received a sobering wake-up call on the serious nature of international cyber threats. States will continue to take a proactive approach to securing our election systems. At the end of the day, we all want Americans to know that votes – and votes alone – will determine the next President of the United States.

Thank you for the opportunity to provide comment.

Secretary of State J. Thomas "Tom" Schedler

Secretary of State Tom Schedler, a resident of Mandeville, was first appointed to the position in 2010 after serving as first assistant for three years. Schedler was then elected by the people to serve a four-year term as secretary of state in 2011.

Schedler has worked diligently to streamline and update the processes within the Secretary of State's Office resulting in a more efficient and effective experience for taxpayers. As a leader who believes the role of the secretary of state is a paternal one, Schedler's priorities include protecting and defending the integrity of every non-partisan election, honoring and preserving the history and symbols of our state and assisting and supporting small businesses in filing their registration forms. A brief summary of Schedler's accomplishments during the last two years in office include:

- **Reducing the number of special elections in Louisiana to preserve limited tax dollars.** After finding Louisiana had twice as many elections as compared to neighboring states over a five year period, Schedler sought new laws to save taxpayer's money and increase the relevance of scheduled elections.
- **Improving voter registration and participation through technology.** Louisiana has the fourth highest voter registration statistics in the nation with 84 percent of eligible voters registered. The nationally recognized GeauxVote Mobile app for smartphones conveniently allows citizens to check their voter registration status, review their individualized ballot in preparation for voting and locate their voting precinct using their phone. Louisiana is the first state in the nation to use this technology. Secretary Schedler recently accepted the 2013 NASS IDEAS Award for the app which recognizes innovation, dedication, excellence and achievement in state member programming by the National Association of Secretaries of State. Additionally, the GeauxVote portal (www.GeauxVote.com) includes a convenient online voter registration component which can be used by citizens statewide, 24 hours a day, 7 days a week. Louisiana was the second state in the country to implement online registration.
- **Honoring the sacrifice of our military servicemen.** The Honor Vets. Vote. Program, encourages voters to visit www.sos.la.gov/honorvets for each election and honor a veteran with their vote. Upon completion of a short form, voters can print a commemorative certificate and are mailed a lapel pin and bumper sticker. Schedler also traveled to the Middle East in 2012 instructing active military servicemen how to vote while overseas.
- **Enhancing services in the commercial division.** Schedler worked to expand www.GeauxBiz.com for businesses wishing to file their corporate forms electronically and recently launched a one-stop online portal for all statewide corporate transactions. The Geaux Biz portal saves small businesses time and money and improves the overall operations of the Secretary of State's Office. Protecting owners through business identity theft legislation was the cornerstone of his first year in office.

Secretary Schedler's solid foundation of governmental and private sector experience includes three terms in the Louisiana State Senate. During that time, he was honored with the Monte M. Lemann Award by the Louisiana Civil Service League (1997), Legislator of the Year by the

Alliance for Good Government (2002), Republican of the Year (2006), the East Baton Rouge Parish Republican Women's Red Pelican Award (2014) and was elected twice by his peers in the Senate to serve as Chairman of the Republican Delegation. In addition, he was recently elected President of the National Association of Secretaries of State (2015-16) after serving for several years as a member of the Executive Board as well as co-chairman for the Task Force on Emergency Preparedness for Elections. He currently serves as an advisory member of the national Election Assistance Commission's (EAC) Board of Advisors in Washington D.C.

Professionally, he is a licensed real estate broker, former bank president and board of directors member and serves on the Board of Trustees for a 156-bed regional hospital and medical center.

Civically, he has participated in numerous organizations including serving as President of the Slidell Rotary Club and is a Paul Harris Fellow. He is also a CASA trained court appointee.

Schedler was born and raised in New Orleans. He graduated from De La Salle High School in 1967 prior to receiving his Bachelor of Science in marketing from the University of Louisiana at Lafayette in 1971. In 1999, he was honored by his high school as one of De La Salle High School's 125 outstanding graduates over the school's first 50 years, and in 2010, was honored with the school's Leadership Award. He has also been honored by his community as Citizen of the Year and Employer of the Year.

Secretary Schedler is married to his wife of 40-plus years, the former Stephanie Gele' of Lafayette. She owns and operates hospice programs in Louisiana and Mississippi. They have three married daughters and four grandchildren.

Chairman SMITH. Thank you, Secretary Schedler.
And, Mr. Becker.

TESTIMONY OF MR. DAVID BECKER,
EXECUTIVE DIRECTOR,
THE CENTER FOR ELECTION INNOVATION & RESEARCH

Mr. BECKER. Good morning, and thank you, Mr. Chairman, and Ranking Member Johnson, for the opportunity to testify today on the important issue of the security of our election system.

My name is David Becker and I'm the Executive Director of the Center for Election Innovation and Research, a nonprofit working in partnership with election officials like Secretary Schedler and technology leaders to improve our system of elections.

My experience in elections goes back about two decades, starting with a seven-year stint as a senior trial attorney with the voting section of the Department of Justice under both the Clinton and George W. Bush Administrations where I observed dozens of elections in hundreds of precincts nationwide and then served for several years as the Director of the Elections Program at Pew where I oversaw efforts to use technology to improve the efficiency and security of elections.

As an initial matter, we should be clear about the election systems that are in place and what they each do and what if any relative vulnerabilities might exist. Voter registration databases or a key election system have been in the news a lot recently. As you noted, there was a breach of the Illinois voter registration database where personal data from several thousand voters appears to have been accessed. In Arizona, it appears the State successfully detected an attempted hack of their state voter registration database and prevented access of any private data.

But in both cases initial investigations suggest no voter data was changed. The voter registration lists remained intact with the primary goal of the hack seemingly being to access personal data for the purposes related to identity theft rather than to manipulate the voter lists themselves.

While we should continue to be vigilant about these centralized databases, to my knowledge, every State creates a regular backup of their voter registration lists, and most States on a daily basis, so that should anything go wrong with the databases themselves, the list could be reconstructed prior to the election.

And while there have also been concerns expressed about the hack of the Democratic National Committee email system, that system is completely different than the election systems in place. That was an attack on a centralized email server and a nongovernmental entity which bears no analogy to the highly regulated systems in place in the States to administer elections.

The voting machines themselves include paper ballots or electronic devices on which votes are cast and include vote tabulation equipment. And with regard to those systems, I can say that while no system is 100 percent hack-proof, elections in this country are secure, perhaps as secure as they've ever been, and that voters should have confidence that their votes will be counted and counted accurately.

There are four primary reasons that voters should feel confident in our election system. First, our election system is highly decentralized. Each State governs the administration of elections independently, and within each State there are many individual election jurisdictions—counties, towns, and the like—totalling approximately 10,000 nationwide that actually administer those elections.

Even within many States, counties use different systems and dozens of different technologies to conduct elections, and within those thousands of election jurisdictions there are well over 100,000 Election Day precincts and polling places where ballots are cast and collected, and that is just on Election Day, not taking into account the thousands of early-voting sites and tens of millions of mail ballots that will be utilized this November. Thus, there isn't a single or concentrated point of entry for a hacker. Rather, there are thousands of points hacker would have to successfully navigate to manipulate the results of a national election.

Second, voting machines are kept securely. These machines are subjected to rigorous protocols for chain of custody and testing in every jurisdiction. Machines are held under lock and key with additional protections in place to ensure that nobody without proper credentials can access the devices. It's exceedingly difficult to gain unauthorized access to even one of these machines and nearly impossible to gain access to more than one. Prior to every election, not just federal elections, but every time the equipment is used, these machines go through a series of tests called logic and accuracy tests to confirm that they are working as intended, recording and tabulating votes accurately.

Third, unlike voter registration databases or email systems, I know of no jurisdiction where voting machines are connected to the Internet. This makes it nearly impossible for a remote hacker, whether in Moscow, Russia, or Moscow, Idaho, to access the equipment and plan malicious code or otherwise hack the system. Without connectivity, it would require a hacker to have unfettered physical access and enough time to sabotage one machine just to impact the results on one device in one polling place. To manipulate election results on a state or national scale would require a conspiracy of literally hundreds of thousands and for that massive conspiracy to go undetected.

Which brings us to the fourth reason: Even if hundreds of thousands of conspirators operated undetected on a diverse range of systems, defeating the testing and chain-of-custody protections in place, it would likely have no effect on the vast majority of election results nationwide because well over 75 percent of voters vote on paper ballots or on a device that creates a paper record.

And in most States—32 plus DC. as of 2014, there is a postelection audit requirement that mandates States match the paper record to the digital record, and if a discrepancy exists, recount the paper ballots for use as the official record. The States that require such an audit include the battleground States of Arizona, Colorado, Florida, Nevada, New Mexico, North Carolina, Ohio, Pennsylvania, Virginia, and Wisconsin, among others, so even if a grand conspiracy were viable, a postelection audit requirement would almost certainly discover it prior to the election results becoming official.

There's been a lot of hyperbole surrounding the selection, but the processes in place to ensure the integrity of our election system should not become part of the political rhetoric. There are few loudly seeking to sow distrust in the system, but there are far more working quietly and collaboratively at the federal, state, and local level and election officials across the political spectrum like Secretary Schedler here who are working to secure our voting systems and reassure voters that the selection will accurately reflect voters' choices.

And voters can play a role as well, by attending pre-election voting machine tests and especially volunteering to serve as poll workers to see the process firsthand, whether it's federal officials offering assistance and resources to the States, state and local officials sharing best practices, or citizens serving as poll workers, this cooperation and diligence will protect our elections in 2016 and safeguard future elections as well.

Thank you and I'd be happy to take any questions.

[The prepared statement of Mr. Becker follows:]

Testimony of David J. Becker

Executive Director, Center for Election Innovation & Research

Before the House Committee on Science, Space, & Technology

September 13, 2016

Good morning and thank you for the opportunity to testify today on the important issue of the security of our election system. My name is David Becker, and I am the Executive Director of the Center for Election Innovation & Research, a non-profit working in partnership with election officials and technology leaders to improve our system of elections.

My experience in elections goes back about two decades, starting with a seven-year stint as a senior trial attorney with the Voting Section of the Department of Justice, working in both the Clinton and George W. Bush administrations. While there, I litigated and enforced federal voting laws including the Voting Rights Act, the National Voter Registration Act, the Help America Vote Act, and the Uniformed and Overseas Citizens Absentee Voting Act.

I then served for several years as the director of the election initiatives program at The Pew Charitable Trusts where I oversaw efforts to use technology to improve the efficiency and security of elections. While there, I led the following initiatives:

- The Voting Information Project, where partnering with Google and other technology companies, we successfully delivered accurate election information to tens of millions of voters across the country, including millions in 2016 alone;
- Successful efforts to expand online voter registration, which has proven to be cost-effective and convenient, from two states in 2008 to over 30 states today;
- Helped found the Electronic Registration Information Center (ERIC), a sophisticated data center with over 20 member states that helps them keep their voter rolls up-to-date, and which so far has helped those states identify over 4 million out-of-date voter records and register almost 1 million new voters;
- Research that brought to light the difficulty military and overseas voters have, which led to the passage of the Military and Overseas Voter Empowerment Act in 2010.

During my time working in elections, I have observed dozens of elections in hundreds of polling places, and had the opportunity to visit many state and local election offices all over the country. In that capacity, I've learned much about the systems the states and counties have in place, and the security processes election professionals employ.

As an initial matter, we should be clear about the election systems in place, what they each do, and what, if any, relative vulnerabilities might exist. Voter registration databases are a key election system and have been in the news a lot recently. As you are aware, there was a breach of the Illinois voter registration database, where personal data from several thousand voter records were accessed. In Arizona, it appears the state successfully detected an attempted hack of their state voter registration database and prevented access of any private data. In both cases, initial investigation suggests no voter data was changed, the voter registration lists remained intact, with the primary goal of the hack being to

access personal data likely for purposes related to identity theft, rather than to manipulate the voter lists themselves. While we should continue to be vigilant about these centralized databases, to my knowledge, every state creates a regular backup of their voter registration lists – in most states on a daily basis – so that should anything go wrong with the databases themselves, the list could be reconstructed easily and quickly. It isn't impossible that the voter lists could be the target of an attack, but those lists are usually closed weeks before the election, with backup copies of the lists available in hardcopy and digitally should any mischief take place.

And while there have also been concerns expressed about the hack of the Democratic National Committee email system, that system is completely different than the election systems in place. That was an attack on a centralized email server, in a non-governmental entity, which bears no analogy to the highly-regulated systems in place in the states to administer elections.

The voting systems include paper ballots or electronic devices on which votes are cast, and include vote tabulation equipment, and with regard to those systems I can say that, while no system is 100 percent hack-proof, elections in this country are secure, perhaps as secure as they've ever been, and that voters should have confidence that their votes will be counted and counted accurately.

There are four primary reasons that voters should feel confident in our election system:

First, our election system is highly decentralized. Each state governs the administration of elections independently, and within each state, there are many individual election jurisdictions – counties, towns, and the like, totaling approximately 10,000 nationwide – that actually administer those elections. Even within many states, counties use different systems and dozens of different technologies to conduct elections. And within those thousands of election jurisdictions, there are well over 100,000 Election Day precincts and polling places where ballots are cast and collected. And that is just on Election Day, not taking into account the thousands of early voting sites, and tens of millions of paper mail ballots that will be utilized this November. Thus, there isn't a single or concentrated point of entry for a hacker. Rather, there are thousands of points a hacker would have to successfully navigate to manipulate the results of a national election.

Second, voting machines are kept secure. These machines are subjected to rigorous protocols for chain of custody and testing in every jurisdiction. Machines are held under lock and key with additional protections in place to ensure that nobody without proper credentials can access the devices. It is exceedingly difficult to gain unauthorized access to even one of these machines, and nearly impossible to gain access to more than one. Prior to every election – not just federal elections, but every time the equipment is used - these machines go through a series of tests called logic and accuracy tests to confirm that they are working as intended, recording and tabulating votes accurately. These tests are open to the public and entirely transparent, so everyone can observe; some jurisdictions even use social media to make sure that their voters can witness the process.

Third, unlike voter registration databases or email systems, I know of no jurisdiction where voting machines are connected to the internet. This makes it nearly impossible for a remote hacker, whether in Moscow, Russia or Moscow, Idaho, to access the equipment and plant malicious code or otherwise hack the system. Voting machines are kept secured, connected to nothing – not even power - until they are tested and used, and then they are under constant observation. Without connectivity, it would require a hacker to have unfettered physical access and enough time to sabotage one machine just to impact the

results on one device in one polling place. To manipulate election results on a state or national scale would require a conspiracy of literally hundreds of thousands, and for that massive conspiracy to go undetected.

Which brings us to the fourth reason. Even if hundreds of thousands of conspirators operated undetected on the diverse range of systems, defeating the testing and chain of custody protections in place, it would still have no effect on the vast majority of election results nationwide. That is because well over 75 percent of voters vote on paper ballots or on a device that creates a paper record. And in most states – 32 plus the District of Columbia, as of 2014 – there is a post-election audit requirement that mandates states match the paper record to the digital record, and if a discrepancy exists, recount the paper ballots for use as the official record. The states that require such an audit include the battleground states of Arizona, Colorado, Florida, Nevada, New Mexico, North Carolina, Ohio, Pennsylvania, Virginia, and Wisconsin, among others. So even if a grand conspiracy were viable, a post-election audit requirement would almost certainly discover it prior to election results becoming official, with the paper ballots then being used as the official ballot of record.

There has been a lot of hyperbole surrounding this election, but the processes in place to ensure the integrity of our election system should not become part of the political rhetoric. I've yet to meet an election official at the state or local level, Republican or Democrat or neither, who was not working as hard as possible to ensure that every election reflects the will of the people, even if the outcome differed from their own political interests. There are a few loudly seeking to sow distrust in the system, but there are far more working quietly and collaboratively, at the federal, state, and local level, to secure our voting systems and reassure voters that this election will accurately reflect voters' choices.

And voters can play a role as well, by attending pre-election logic and accuracy tests, and especially, volunteering to serve as poll workers to see the process first hand. Whether it is federal officials offering assistance and resources to the states, state and local officials sharing best practices, or citizens serving as poll workers, this cooperation and diligence will protect our elections in 2016 and safeguard future elections as well.

David J. Becker

Executive Director

The Center for Election Innovation & Research

www.electioninnovation.org

dbecker@electioninnovation.org

David Becker is the Executive Director and Co-Founder of the Center for Election Innovation & Research, leading this cutting-edge non-profit's work to improve election administration through research, data, and technology. David created CEIR to be the first effort of its kind, with a proven track record of working with election officials and experts from around the country and across the aisle. Through its efforts, CEIR seeks to reverse the historical decline in voter turnout, and give election officials the tools they need to ensure that all eligible voters can vote conveniently in a system with maximum integrity.

Prior to founding CEIR, David was Director of the elections program at The Pew Charitable Trusts, driving reforms in election administration, including using technology to provide voters with information they need to cast a ballot; assessing election performance through better data; and upgrading voter registration systems. As the lead for Pew's analysis and advocacy on elections issues, David spearheaded development of the innovative Electronic Registration Information Center, or ERIC, which to date has helped a bipartisan group of nearly two dozen states correct almost 4 million out-of-date voter records, and led to these states registering almost a million new eligible voters. David led campaigns in dozens of states, red and blue and everything in between, and directed Pew's partnerships with state government agencies, and with private sector partners like Google, IBM, Facebook, and others.

Before joining Pew, David served for seven years as a senior trial attorney in the Voting Section of the Department of Justice's Civil Rights Division, where he led numerous investigations into violations of federal voting laws regarding redistricting, minority voting rights, voter intimidation, and vote dilution. During his time at the Justice Department, David worked in dozens of states enforcing federal election laws and observing elections in thousands of precincts, and served as lead trial counsel in many cases, including Georgia v. Ashcroft.

David's appearances in the media include *The New York Times*, *The Washington Post*, MSNBC, and NPR, and he has been published several times, including by the Stanford Social Innovation Review, the University of California, Berkeley, and The Hill.

David received both his undergraduate and law degrees from the University of California, Berkeley.

Chairman SMITH. Thank you, Mr. Becker.
And, Dr. Wallach.

TESTIMONY OF DR. DAN S. WALLACH, PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND RICE SCHOLAR, BAKER INSTITUTE FOR PUBLIC POLICY, RICE UNIVERSITY

Dr. WALLACH. Chairman Smith, Ranking Member Johnson, Members of the Committee, it's a great honor to speak to you today about our nation's voting systems and the threats they face this November and the steps we might take to mitigate those threats.

My name is Dan Wallach. I've been a Professor in the Department of Computer Science at Rice University in Houston for 18 years. And my main message for you here today is that our election systems face credible cyber threats from our nation-state adversaries, and it's prudent to adopt contingency plans before November to mitigate these threats.

In particular, we've learned that Russia may have been behind leaked DNC emails for the explicit purpose of manipulating our elections. We've also learned of attacks on voter registration databases in Arizona and Illinois, and that's only the ones we know about. There might be more.

We must prepare for the possibility that Russia or other sophisticated adversaries will use their cyber skills to attack our elections, and they need not attack every county in every State. It's sufficient for them to go after battleground States where a small nudge can have a large impact. The decentralization that we've heard about is helpful but it's not sufficient.

My number one concern is our voter registration databases because they are online, and if an attacker can damage or destroy the voter registration databases, they could disenfranchise a significant number of voters, leading to long lines and other difficulties. The provisional voting process requires filling out affidavits, it's slow, it takes time, and that wouldn't work for million voters.

Paperless electronic voting systems and their tabulation systems are also vulnerable. Despite not generally being connected to the Internet, these systems were unfortunately never engineered with security in mind, and expert analyses by myself and others have found unacceptable security issues.

Our biggest nation-state adversaries have the capability to execute attacks against these systems. For example, Russia was behind an attack of this kind directed at Ukraine's 2014 election where a hacked tabulation system would have reported results favorable to Russia. The Ukrainians were lucky enough to catch this.

Our options between now and November are largely limited to contingency planning. If we're lucky, we might detect attacks before Election Day, but it's important to make plans now for recovering from unforeseen cyber disasters in the same way that we make plans for natural disasters, including running drills and exercises and having plans written out and thought through.

If, for example, we were to conclude on Election Day that our computer systems had been unreliable, a contingency plan might be to rapidly print millions of paper ballots and rerun the election the next day. Legislation passed in most States following 2012's

Hurricane Sandy appears to allow for such mitigations. The details vary State to State.

Between now and November we should also be aggressive at deploying expert teams to do security audits of relevant networks and systems particularly in battleground States. If something has been hacked, the sooner we know about it, the better. And my understanding is a critical infrastructure designation would allow States to request assistance from the Federal Government in this role.

We must also plan for the next few years after November's election is complete. Roughly 1/3—we've heard today—we've also heard 1/4. I'm not sure what the real number is. Roughly 1/3 of American voters this fall will use aging electronic voting systems with proven insecure designs. Some new hybrid voting system designs with electronic user interfaces and printed paper ballots are being designed by Los Angeles County, California, and Travis County. That's Austin, Texas. These have the potential to substantially reduce costs and improve the security of our elections. Federal support could advance their deployment nationwide, and if we do nothing, keeping our aging systems in service holds our elections at risk.

As a quick note, our immediate future should not include Internet voting. It's hard enough to protect the online systems that we already have. Moving additional voters online increases the risks. Traditional hand-marked paper ballots and these new hybrid systems from Los Angeles and Austin are our best paths forward.

As Don Rumsfeld once said, you go to war with the army you have, not the army you might want or wish to have at a later time. We face a similar situation this November with our systems for voter registration casting and tabulation. None of them are ready to rebuff attacks from our nation-state adversaries, nor can we replace them in time to make a difference.

Despite this, we can pursue a number of pragmatic steps such as verifying the integrity of election database backups, and we can make contingency plans for how we may respond if and when we do detect attacks against our elections. If we can somehow determine that tampering with an election voting system did take place, we should have plans in place to print paper ballots or otherwise keep the election going. The sooner we can create and agree on these plans, the more resilient our elections will be to foreign attack.

And even if nothing goes wrong and all this turned out to be nothing but hot air, we should treat these events as a warning. With modest investment, we can improve our practices and replace obsolete and insecure equipment, defeating future attacks like this before they ever get off the ground.

Thank you.

[The prepared statement of Dr. Wallach follows:]

Testimony of Dr. Dan S. Wallach
Professor, Department of Computer Science
Rice Scholar, Baker Institute for Public Policy
Rice University, Houston, Texas

Before the House Committee on Space, Science & Technology Hearing,
"Protecting the 2016 Elections from Cyber and Voting Machine Attacks"

September 13, 2016
Rayburn House Office Building, Room 2318

Chairman Smith, Ranking Member Johnson, members of the committee, it's an honor to speak to you today about our nation's voting systems, the potential threats they face this November, and the steps we might take to mitigate these threats.

My name is Dan Wallach. I've been a professor of computer science at Rice University, in Houston, Texas, for 18 years. My research considers a variety of computer security topics and I've published over 100 papers in the field. Among other honors, I recently served from 2011-2015 on the Air Force Science Advisory Board. I've included a more detailed biography in my written materials. My main message for you here, today, is that our election systems face credible cyber-threats; it's prudent to adopt contingency plans before November to mitigate these threats.

I've maintained a research interest in electronic voting systems starting with their widespread adoption in the early 2000s. In particular, I led an NSF-funded research center, ACCURATE (A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections)[1] from 2005-2011. I also participated in the 2007 California "Top to Bottom Review" of its electronic voting systems, where we found unacceptable security vulnerabilities in every system we studied[2]; those systems were replaced in California with more secure, paper-based systems but are still being used elsewhere and are likely still quite vulnerable. One of my ongoing projects is helping the Travis County (Austin, Texas) Clerk's office design a new electronic voting system to replace their current, aging system[3]. In short, my experience makes me very familiar with how our election systems are vulnerable and how our adversaries might seek to exploit them.

First, I'd like to address the threat. We've learned that foreign nation-state actors, likely Russian, broke into DNC computers and released documents for expressly partisan purposes[4]. So far as we know, they're doing this to manipulate the outcome of November's election. We must ask ourselves the same sorts of questions that arise in any security analysis. Does the adversary have the *means*, *motive*, and *opportunity* to have their desired effect, and do we have the necessary *defenses* and/or *contingency plans* to mitigate these threats?

---

[1] http://accurate-voting.org/
[2] http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/
[3] https://www.usenix.org/conference/evtwote13/workshop-program/presentation/bell
[4] See, e.g., Lichtblau's article in the *New York Times* (July 29, 2016). http://www.nytimes.com/2016/07/30/us/politics/clinton-campaign-hacked-russians.html

It's important to note that this has happened in elections before. Russian hackers, who may or may not have been government-affiliated, committed "wanton destruction" upon Ukrainian election systems in 2014, arranging for the vote tallying system to report incorrect results[5]. The Ukrainians were lucky to catch this; it's not uncommon for nation-state computer attacks to go unnoticed for months or years. Like the Ukranians in 2014, we face similar vulnerabilities today.

I've written about these issues in a detailed series of blog posts[6] which I'll summarize for you here. **Our biggest vulnerabilities are our voter registration databases**, typically maintained online, so therefore reachable by our adversaries. Web sites with databases are ubiquitous and their vulnerabilities are well-understood to cyber threat actors. Every university computer security class has its students learn to attack and defend these sorts of things. While a defender must eliminate all possible attacks, an attacker needs only find a single weakness, so it's reasonable to expect these weaknesses exist in our voter registration systems. **We can and should expect our adversaries to go after voter registration systems**, and there's evidence of this already having happened in Arizona and and Illinois[7] [8]. The partisan impacts are easy to envision. You can selectively disenfranchise voters by deleting them from the database or otherwise introducing errors. How can you infer voter partisanship? Political campaign managers use a variety of predictive models for targeted mailings, get-out-the-vote campaigns, and so forth; we can expect adversaries to do the same. **Can we mitigate against these threats?** First and foremost, we can require computer backups and run drills to make sure we can rapidly recover from corruption. To detect and deter more sophisticated adversaries, we should deploy state-of-the-art intrusion detection and prevention systems in "battleground" counties and states. Furthermore, we already have "provisional voting," allowing voters to cast a ballot, despite their absence from the database, but provisional voting procedures are meant to handle a fairly small number of voters. If a substantial fraction of voters had to vote provisionally, doing the necessary paperwork, the process would grind to a halt. Long lines disenfranchise voters. Provisional balloting also doesn't work very well in states heavily

[5] Clayton, "Ukraine election narrowly avoided wanton destruction from hackers", *Christian Science Monitor* (June 2014), http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video

[6] https://freedom-to-tinker.com/blog/dwallach/election-security-as-a-national-security-issue/ and https://freedom-to-tinker.com/blog/dwallach/a-response-to-the-national-association-of-secretaries-of-state/

[7] Isikoff, "FBI says foreign hackers penetrated state election systems", *Yahoo! News* (August 29, 2016), https://www.yahoo.com/news/fbi-says-foreign-hackers-penetrated-000000175.html

[8] Nakashima, "Russian hackers targeted Arizona election system", *Washington Post* (August 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

utilizing vote-by-mail ballots (e.g., California, Colorado, Nevada, Oregon and Washington State), where voters might not even realize their ballots are missing. We might be able to use traditional printed paper pollbooks, rather than electronic pollbooks, but these don't work easily with either early voting or election day vote centers, where many thousands of different ballot styles must be available to thousands of voters.

Can our adversaries get malware into our voting machines, themselves? The U.S. military protects its important secrets by keeping them on distinct networks and servers, physically separated from the Internet. This "air gap" defense is also used to protect voting machines. Despite this, voting machines still interact with normal computers as part of their initialization phase (loading software and ballot definitions) and the tabulation phase (extracting cast-vote records and computing the totals). Even if the whole process is designed to be "air gapped" from the Internet (and it absolutely must be air-gapped), nation-state adversaries have devised a variety of workarounds. The Stuxnet malware, for example, was engineered specifically to damage nuclear centrifuges in Iran, even though those centrifuges were never connected to the Internet. We don't know exactly how the Stuxnet malware got in, but it did nonetheless[9]. Combine the patience and resourcefulness of a nation-state adversary with the unacceptably poor state of security engineering in our voting systems, and especially if we consider the possibility of insider threats, then yes, it's entirely reasonable to consider attacks against our voting systems to be within the feasible scope of our adversaries' capabilities. The best mitigations we have for systems that we use today are only feasible where we have paper ballots. The mere *possibility* of a recount or audit of the paper ballots acts as a deterrent to an electronic attack; it's much more difficult to tamper with paper, in bulk, relative to the effort to tamper with purely electronic records, as used in a number of states including the battleground states of Pennsylvania and Georgia. Conversely, if our paperless electronic voting systems were attacked, we'd be unlikely to see evidence of it in the voting machines or tally systems.

Does an adversary need to attack everywhere? Our adversaries understand how the American political system works. They know about "battleground states". They can focus their efforts on states where a small nudge might have a large impact. Also, consider that our adversaries might have a variety of goals. If they simply want to disrupt our elections, and if they're unconcerned with attribution, then even very modest or crude attacks will raise doubts and damage voter confidence in the election outcome. Trust in our election systems is fragile and is potentially easily shaken by our adversaries.

---

[9] For more details, see, e.g., Langner et al. (2013). http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

What can we do between now and November? It's far too late to change the technologies upon which we will cast our votes. My best advice is that we need *contingency planning*. Four years ago, when Hurricane Sandy disrupted elections in several northeastern states, this was a big topic of discussion[10]. The National Association of Secretaries of State prepared a summary of relevant statutes in every state[11]. In many respects, cyber activities from a nation-state adversary are similar to natural disasters in the impact they can have on our elections. What can you do if your voter registration database has been destroyed? Perhaps try to restart things from a backup. What can you do if your electronic voting systems refuse to turn on? Perhaps make an advance arrangement with a print-shop to rush a large order of paper ballots if need be. What if we have no direct evidence of tampering but we have credible intelligence reports that suggest otherwise? Many state statutes already allow governors to declare states of emergency and take appropriate actions up to and including re-running the election on a different day. In short, we must prepare for a disaster, while hoping it may never occur.

When we talk about nation-state adversarial attacks on computer networks, we often use the term "advanced persistent threat" (APT), indicating that these adversaries are good at hiding and at sticking around despite efforts to remove them. While it's helpful and important to apply software updates, use good passwords, properly configure firewalls and intrusion detection systems, and otherwise practice "good hygiene", the process of detecting and removing an APT adversary is complicated. A number of companies and consultancies have begun offering products and services that help in this area, and state and county office should hire such companies to audit and remediate their systems, particularly in "battleground" states, although this may require financial assistance from the Federal government.

How do we make sure we won't face these risks in subsequent elections? The 2002 Help America Vote Act had two parts. It allocated money to replace obsolete voting equipment and it created the Election Assistance Commission (EAC) which, among other things, absorbed the voting systems standards-making process which was previously managed by the National Association of State Election Directors (NASED). The problem was that the money was allocated to the States before the EAC was up

---

[10] See, e.g., Kaplan in the *New York Times* (November 12, 2013) http://www.nytimes.com/2013/11/13/nyregion/lessons-from-hurricane-sandy-being-applied-to-election-planning.html

[11] http://www.nass.org/elections-voting/nass-task-force-on-emergency-preparedness-for-elections/. See also, Wall, *Preventing Disasters from Disrupting Voting: National Task Force Urges States To Plan for Election Emergencies* (October 15, 2014) http://knowledgecenter.csg.org/kc/content/preventing-disasters-disrupting-voting-national-task-force-urges-states-plan-election

and running; the vendors who had products for sale at the time were able to sell these inadequate products as-is and had neither the incentives nor ability to improve them. Now, a over decade later, many of these systems are nearing the end of their usable service life. Their aging hardware is starting to break down. What should we buy next time to make sure we don't have these problems again? I see two options:

Next-generation optical scan systems: The big elections equipment vendors are all now selling "precinct-based optical scan systems" (PCOS), as shown in Fig. 1, where paper ballots are marked by hand and scanned at the ballot box. These systems offer features to catch some kinds of voter errors[12], allowing voters a chance to remake their ballot. Optical scan systems face all the same electronic tampering threats from adversaries, but these threats can be mitigated by robust paper auditing procedures. California piloted such audits in 2011-2013 and submitted a variety of recommendations to the EAC[13], presently also part of California and Colorado state laws. In short, by randomly selecting a small number of paper ballots and comparing those to their corresponding digital records, you can mathematically determine that if you were to actually do a full recount -- that is, count all the paper ballots -- the results would not differ between a hand count and the electronic count. Not only does this help with accuracy, it also mitigates against malicious software tampering, because such tampering would introduce discrepancies that the audit would detect.

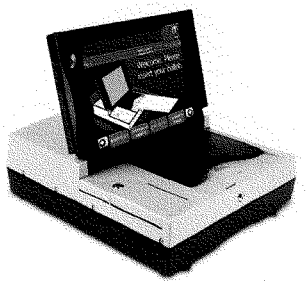


Fig. 1: ES&S DS200, precinct-based optical scanner with on-screen assistance features.

[12] The two primary forms of "voter error" that we can detect in a scanner are "overvotes", wherein a voter selects more than one candidate for a given election contest, and "undervotes", wherein a voter selects no candidates for a given contest.

[13] http://www.sos.ca.gov/elections/voting-systems/oversight/post-election-auditing-regulations-and-reports/post-election-risk-limiting-audit-pilot-program/

Next-generation hybrid voting systems: The two most exciting developments aren't coming from the commercial voting system vendors but instead from election officials in Los Angeles County, California and Travis County (Austin), Texas. The LA Voting Systems Assessment Project (VSAP)[14], as seen in Fig. 2, and the Travis County STAR-Vote (Secure, Transparent, Auditable, Reliable) system[15] both use large touch-screen computers which can accommodate complex ballot designs with multiple languages and both offer sophisticated accessibility features. Both generate printed paper ballots which can be tallied electronically and audited manually. Both use sophisticated cryptographic techniques to protect the system.

Fig. 2: Los Angeles VSAP prototype, with button-box, touch-screen, and printer.

I've been working more closely with Travis County than Los Angeles, so I can tell you that Travis County has allocated $4 million to start their procurement process shortly; they expect they will ultimately spend around $12 million before they can begin testing in real elections in 2019. If they had additional funds now, they could advance their timeline and have a more full-featured system.

Both Travis and Los Angeles Counties envision their systems will use open source software, reducing ongoing support and maintenance costs. These projects have the potential to see widespread nationwide

[14] http://vsap.lavote.net/
[15] http://traviscountyclerk.org/eclerk/Content.do?code=E.34

adoption, which would make elections far more resilient to cyber attacks than with the voting systems currently on the market.

Internet voting: While it's not directly relevant to today's hearing, somebody will inevitably propose Internet voting as a solution to every problem in voting.

Why can't we just vote on the Internet? While it's attractive to imagine the convenience of online voting, the Internet also makes it much easier for nation-state adversaries to attack our elections. In one prominent example, Washington DC conducted a pilot election using an Internet voting system, inviting external researchers to have a go at attacking them. The University of Michigan's Prof. Alex Halderman and his students managed to completely compromise this system in a few hours[16]. They were able to watch election workers from the internal video cameras. They arranged for fictional characters to win all the elections. They even modified the web site to play the Michigan fight song after each vote was cast. If Prof. Halderman and his students can do this, so can our adversaries. Halderman and others have studied Internet-based voting systems in New South Wales, Australia[17], and in Estonia[18], finding similar problems. Safe internet voting is simply not feasible today. Instead, we need paper ballots or hybrid systems.

But we can do banking on the Internet! Companies that engage in electronic commerce make significant, ongoing investments in the security of their operations. Despite those investments, their losses are significant:

> In 2015, the British insurance company Lloyd's estimated that cyber attacks cost businesses as much as $400 billion a year, which includes direct damage plus post-attack disruption to the normal course of business. Some vendor and media forecasts over the past year put the cybercrime figure as high as $500 billion and more.[19]

---

[16] Wolchok et al., "Attacking the Washington D.C. Internet Voting System", Proc. 16th Conf. on Financial Cryptography & Data Security (February 2012), https://jhalderm.com/pub/papers/dcvoting-fc12.pdf
[17] Halderman and Teague, "The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election" (June 2015), http://arxiv.org/abs/1504.05646
[18] Springall et al, "Security Analysis of the Estonian Internet Voting System", ACM CCS (Nov. 2014), https://jhalderm.com/pub/papers/ivoting-ccs14.pdf
[19] Morgan, "Cyber Crime Costs Projected To Reach $2 Trillion by 2019", *Forbes* (Jan. 2016), http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/

We can't afford fraud in elections. We can't simply write it off as a cost of doing business. Furthermore, in banking, if a fraudulent transaction occurs, perhaps because a credit card number was stolen, the victim will see it on their statement and can dispute it. In sharp contrast, if an Internet vote was flipped, current systems give the voter no evidence with which discover this. (We don't want voters to have "receipts" indicating how they voted, because that would enable bribery and coercion. Voter privacy is necessary for a secret-ballot election.)

*Will we **ever** be able to vote on the Internet?* Eventually, yes, but definitely not with today's computers, and not on today's internet. This is an open research challenge which requires better security across the board, from consumer operating systems and web browsers through our networks and cloud infrastructure. Internet voting is a great aspirational goal, but it's not feasible yet to do this, particularly in light of the threats these systems will face.

Can't we use sophisticated cryptography, as in the Bitcoin blockchain? Bitcoin is an electronic currency with a global "shared ledger" that has some interesting security properties. Some people have even proposed that we can use it to cast ballots, since casting a ballot for a candidate is superficially similar to sending a "coin" to that candidate. This isn't the venue for a detailed technical critique, but suffice to say that we've included blockchain-like techniques in Travis County's STAR-Vote, and that cryptographic techniques don't magically eliminate the dangers of having a voting system online and accessible to our nation-state adversaries. Furthermore, it's important that our election integrity not rely solely on intangible mathematics. There must also be tangible evidence that can be understood without an advanced degree. That tangible evidence must be paper ballots.

How can we better enable our overseas and military voters to cast their ballots? Many overseas voters complain that postal ballot delivery and return is slow and unreliable. The current state of the art process is delivering ballots digitally where the voter prints them, marks them by hand, and returns them in the postal mail. In some cases, military ballots are returned by fax, printed, and then mailed domestically. This process is a mess and we owe a better solution to our overseas and military voters. Rather than Internet voting, what we really need is some form of *remote kiosk voting*, where overseas voters can go to a nearby embassy, consulate, or military base. There's a clear role here for NIST and the EAC to standardize these things, making it easier for a remote voter to cast a private vote in a controlled polling location.

Conclusions

As Don Rumsfeld once said, "you go to war with the army you have, not the army you might want or wish to have at a later time." We face a similar situation this November with our systems for voter registration, casting, and tabulation. None of them are ready to rebuff attacks from our nation-state adversaries, nor can we replace them in time to make a difference. Despite this, we can pursue a number of pragmatic steps, such as verifying the integrity of election database backups, and we can make contingency plans for how we may respond if and when we do detect attacks against our elections. If we can somehow determine that tampering with an electronic voting systems took place, we should have plans in place to rapidly print paper ballots and bring the voters back to the polls. The sooner we can create and agree on such plans, the more resilient our elections will be to foreign attacks. And even if nothing goes wrong and all this turned out to be nothing but hot air, we should treat these events as a warning. With modest investments, we can improve our practices and replace obsolete and insecure equipment, defeating future attacks like this before they ever get off the ground.

One Page Summary

Our elections face a credible threat. We've learned that Russia may have been behind leaked DNC emails, explicitly to manipulate our elections. We've also learned of attacks on voter registration databases in Arizona and Illinois. We must prepare for the possibility that sophisticated adversaries will use their "cyber" skills to attack our elections. And they need not attack every county in every state. It's sufficient for them to go after "battleground" states, where a small nudge can have a large impact.

Voter registration databases are particularly vulnerable because they're online. If an attacker can damage or destroy our voter registration databases, they could disenfranchise significant numbers of voters, leading to long lines and other difficulties.

Paperless electronic voting systems, and their tabulation systems, are also vulnerable. Despite not generally being connected to the Internet, these systems were never engineered with security in mind, and expert analyses have found unacceptable security issues. Our biggest nation-state adversaries have the capability to execute attacks against these systems.

Our options between now and November are largely limited to contingency planning. If we're lucky, we might detect attacks before Election Day, but it's important to make plans for recovering from unforeseen cyber disasters in the same way that we make plans for natural disasters, including running drills and exercises. If, for example, we were to conclude that our computer systems were unreliable, a contingency plan might be to rapidly print millions of paper ballots and rerun the election. Legislation passed in most states following 2012's Hurricane Sandy generally allows for such mitigations.

We must also plan for the next few years, after November's election is complete. Roughly one third of American voters this fall will use aging electronic voting systems with proven insecure designs. New hybrid voting systems, with electronic user interfaces and printed paper ballots, are being designed by Los Angeles County, California and Travis County (Austin), Texas. These have the potential to substantially reduce costs and improve the security of our elections. Federal support could advance their deployment nationwide. If we do nothing, keeping our aging systems in service holds our elections at risk.

Our immediate future should not include Internet voting. It's hard enough to protect the online systems that we already have. Moving additional voters online will only make things worse. Traditional, hand-marked paper ballots and the new hybrid electronic systems are our best paths forward.

Biography

Dan S. Wallach is a Professor in the Department of Computer Science and a Rice Scholar at the Baker Institute for Public Policy at Rice University, where he has been for 18 years. His research considers a variety of topics in computer security, including electronic voting systems security, where he served as the director of an NSF-funded multi-institution research center, ACCURATE (A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections), from 2005-2011. He has also served as a member of the Air Force Science Advisory Board (2011-2015) and the USENIX Association Board of Directors (2011-2013).

Wallach earned his M.A. (1995) and PhD (1999) from Princeton University, advised by Profs. Edward Felten and Andrew Appel. He earned his B.S. EE/CS from the University of California, at Berkeley (1993).

Chairman SMITH. Thank you, Dr. Wallach.

I'll recognize myself for questions. And, Dr. Wallach, let me address the first one to you. You raised a lot of interesting issues. I guess my question is where do you think our election systems are the most vulnerable? What are the one or two areas that we'd need to guard against?

Dr. WALLACH. So I believe my top concern is the voter registration systems because they are generally online, and if it's online, it's accessible from the Internet, and if it's accessible from the Internet, it's accessible from our nation-state adversaries.

And as I mentioned before, if you can either selectively or entirely delete people who you'd rather not vote, the current provisional voting system can't really scale to support a large number of voters who are filling out affidavits and following that process.

My second concern is the vote tabulation systems. Generally speaking, these tend to be old computers running old operating systems, in some cases Windows 2000 where security patches aren't even available from the vendor anymore, and that means that there are significant vulnerabilities where attacking a single point could result in an interesting result.

Chairman SMITH. Okay. Thank you, Dr. Wallach.

By the way, when I hear you all recommend paper ballots, I wince a little bit because those of us from Texas have sometimes read about what happened in the 1950s where a ballot box was stuffed with paper ballots and it changed the outcome of a Senate race and perhaps elected the next President. So I sometimes worry about paper ballots as well.

Let me address a question to all the panelists here today. And we've heard about some of the vulnerabilities. Let me ask you to rate on a scale of one to five with five being the most vulnerable, the most at risk, where you think we stand both in this election, and let's take the long view—say this election and the next election—how vulnerable are we to being hacked, not necessarily successfully hacked, but how likely is it that there will be attempts to interfere in our elections process by foreign countries this election or the next? And again one to five with five being the greatest risk.

Dr. Romine?

Dr. ROMINE. It's a little hard for me to answer that question principally because it involves intent of malefactors, and I don't really have any background to be able to determine the level of intent.

Chairman SMITH. Okay. Let's assume, then, how likely is it that there would be intentional attempted hacking in the next two elections? If you want to use——

Dr. ROMINE. It's not unreasonable to imagine attempts. In fact, as others have testified, there have been a couple of attempts to hack into voter registration systems currently. I think most CIOs at most organizations will tell you that there's a sort of constant current of probing of their IT systems. And so with respect to voter registration, I would say the possibility that an attempt could be made is not out of the question.

With respect to the voter—the——

Chairman SMITH. Maybe I should say likely or unlikely, would you consider that to be an easier way to describe it or not?

Dr. ROMINE. It's still difficult for me to answer that question, but I would say I would put it somewhere in between. I can't say that it's likely but I can't rule it out either.

Chairman SMITH. Okay. Thank you.

Secretary Schedler?

Mr. SCHEDLER. I'll take a stab at that. I'll say on the registration side of it, as evidenced by the two States that have had a problem, one of which, from what I understand the code was giving and the other one was detected immediately. I'd probably give it around a three. On the Election Day, one and one half or two.

Chairman SMITH. Okay. Good. Thanks. Mr. Becker?

Mr. BECKER. Yes, I agree. I think it's not out of the realm of possibility that there will be an attempted hack either before the election or at any time, as there was with the voter registration databases. But I think the chance that it would be successful is down below two. I think vigilance is important but it appears that the primary goal here is to disrupt confidence in the election rather than actually manipulate election results.

Chairman SMITH. So likely attempt, unlikely success?

Mr. BECKER. Correct.

Chairman SMITH. Okay. Dr. Wallach?

Dr. WALLACH. So in the cybersecurity lingo we often have this phrase "advanced persistent threat" that we use as a colloquial way of talking about nation-state adversaries who have patience and skills and will take the time, might do something years in advance. It's often the case that adversaries are present in very secure and highly protected networks for months at a time before they're detected.

So trying to rank these vulnerabilities, I'm going to rank them relative to access. I think our voter registration systems are most accessible so I'm most worried about them. I'm secondarily concerned about the tabulation systems, and then I'm concerned about the voting systems themselves, particularly the paperless electronic ones.

Chairman SMITH. Okay.

Dr. WALLACH. It's very hard for a remote Internet attacker to overwrite printed paper.

Chairman SMITH. Okay. A final quick question, what more should the Administration be doing to protect us from foreign countries attempted hacking of our election systems? Anybody?

Dr. WALLACH. So I think the short answer is providing available expertise and teams to go and do intrusion detection, network monitoring, and other appropriate tasks to just go looking for it.

Chairman SMITH. Okay. My time is up. Any other quick responses to what more the Administration could be doing?

Mr. SCHEDLER. Well, I think with we should be looking more long-term with additional dollars to improve the States' machinery or equipment at this time. It's been over ten years since we did HAVA funding. And I do want to make one comment. As far as Homeland Security assisting us, we already have that assistance through FBI and Homeland Security, and you nearly asked, you don't have to be a critical infrastructure to get that service.

Chairman SMITH. Okay. Thank you.

The gentlewoman from Texas, Ms. Johnson, is recognized for her questions.

Ms. JOHNSON. Thank you, Mr. Chairman.

I take all concerns and challenges over cybersecurity in our elections very seriously. At the same time, we face many other challenges to ensuring that every vote counts and we count every vote. Some of these challenges are the direct results of human action such as related to old technology, and as we've seen in elections past, we even face risks from natural events such as major storms. I'd like each of you to comment on how you would rate the current cybersecurity risk in our upcoming election as it relates to other issues.

Dr. ROMINE. Congresswoman Johnson, from my perspective my entire orientation or the orientation of my organization is looking at the cybersecurity risks and threats, and so all of the other things that you've talked about are really sort of outside of our purview with perhaps one exception, which is that contingency planning that the States and other jurisdictions and the local jurisdictions are encouraged to do under the voluntary voting system guidelines can also protect again these other kinds of natural disasters and other kinds of things that you referenced.

Ms. JOHNSON. Thank you.

Mr. SCHEDLER. Yes, ma'am. I would put that risk again, as I indicated earlier, on Election Day very low for the reason that no State is on the Internet. I find it difficult to hack something that's not on the Internet. All machines are not—none of the machines are linked together. They're all separate cartridges, so they're independent. My bigger concern on Election Day would be something of a physical nature, a physical threat that would be something much more difficult to deal with. And I put that at a very high number.

But as far as cyber attack other than what's occurred on the election side—and again, there's been no change. I think that was more of a data collection attempt personally. I know in Louisiana if you go—we are an online registration State, Ms. Johnson. If you went into my system to change party affiliation, address, whatever you may do, you may think you're accessing my entire system. You're not. You're in a silo and a person behind the scenes drags out that information, disseminates it to the local register and puts it in the public side, the campaign side, or in the registration side. So if someone hacked you, they would only hack Ms. Johnson. They wouldn't get the entire list.

Mr. BECKER. Yes, I agree with that. I think, as Secretary Schedler noted, election officials are on high alert, and they're on high alert not just for this election. They're on high alert for every election. And, you know, in many States if it's Tuesday, it's Election Day because there are so many elections now.

So not only are they trying to make sure that the security of the systems are in place and that the process as a whole is secure but they're also doing, I think, a remarkably good job—probably better than ever before—of balancing that with access to all eligible voters to make sure they can have a good experience.

So whether it's more people having access to easy ways to register to vote, more people having easy access to voting information

like things with the GeauxVote app in Louisiana and many other States or more voters than ever before having access to early voting and mail voting option, I think election officials around the country, both Democrats and Republicans, are doing a remarkably good job, probably better than ever before, balancing out the access and security concerns.

Dr. WALLACH. At the end of the day we need to worry about every problem. We have to worry about hurricanes, we have to worry about earthquakes, and we have to worry about cyber issues and we need to have plans in place to deal with them all. And the interesting thing is if you have plans in place for an earthquake, the earthquake doesn't really care. It's going to happen or not. But if you have plans in place for cyber, you can actually dissuade a cyber attack. If your adversary knows it's not going to work, then they're not going to bother. So I think it's important to do the planning and the forward thinking to make this not be a problem in the future.

Ms. JOHNSON. Thank you very much.

Another real quick question—I know my time is running out. We would all agree that making it easier to participate in our democratic elections process should be a priority. Registering to vote and casting a vote shouldn't be an extra burden for those who can't leave their homes or for people with three jobs and for a family of caregivers. How do we balance our efforts to make voting more accessible with the necessity of having secure elections?

Dr. ROMINE. I'd like to take a slightly different tack. We've actually worked with the Election Systems Commission on accessibility issues and usability issues with regard to voting systems so that people who have physical disabilities, whether it's vision impairment or mobility impairment or other things, do have access to voting systems that they can also use. And one of the advantages of electronic voting systems, as they're being rolled out, is that we can improve the accessibility over paper and pencil, for example.

Mr. SCHEDLER. First off, we do have early voting, certainly something in the last decade that we didn't have prior to that, a paper ballot, relaxed paper ballot laws now. I mean, we all remember the days you used to have—almost have to have a doctor's note or an airline ticket to be able to absentee vote. That's no longer the case across the United States. And we do have easy accessibility through nursing home programs, ADA compliant with visually impaired and the like. So I think there's been tremendous improvements made, and voting is probably easier today than it's ever been.

Mr. BECKER. Yes, I think thanks to the efforts of state and local election officials all around the country and efforts of the Election Assistance Commission and the Presidential Commission on Election Administration and many others, voting is easier today than it ever has been before. As I noted, more people have access to easy voter registration options. Many States—20 States, including Louisiana, have joined the Electronic Registration Information Center, which allows them to keep their voter registration data up-to-date and has resulted in registering about a million—almost a million new voters.

More people have access to voting information and convenience voting options where they can vote by mail or vote early. That trend has been remarkable, and I think we're going to see and I hope that we're going to see the benefits of it in this election and as it expands in many years to come.

Dr. WALLACH. So we've heard about early voting and Election Day vote centers. An interesting thing going on in Travis County—it's Austin, Texas—every single precinct can handle any voter from the whole county. They did that because of redistricting. It was to avoid chaos. But it has the interesting benefit that you can vote near where you work rather than near your home. So I think that there's a lot of opportunity for creative expansion of the availability to vote without making radical changes in how we vote.

Ms. JOHNSON. Thank you very much, Mr. Chairman.

Chairman SMITH. Thank you, Ms. Johnson.The gentleman from California, Mr. Rohrabacher, is recognized for his questions.

Mr. ROHRABACHER. Thank you very much. And thank you, Mr. Chairman, for holding this hearing. I didn't expect it would be as interesting as it's been, so thank you to the witnesses as well.

Let me just start off with one question in terms of getting a sense of information here on one issue the broader issue of whether or not the integrity of our voting process and our election system will be maintained is really vital to the very nature of our country. I mean, this goes to the heart of whether or not we are who we say we are. If we don't have an election process that has integrity, we don't have an election process.

First let me ask this. How many examples do we have of where the Russians have actually—or Russian-based, whoever it is in Russia, have hacked in to our election system?

Mr. SCHEDLER. I know of none. And to be quite honest with you, I ask the question to Secretary Johnson of Homeland Security, is there an imminent threat known? And his answer was no, and that was reported in several news agencies. So I know of zero.

Mr. ROHRABACHER. Does anybody disagree?

Mr. SCHEDLER. I had a request from a Russian Embassy out of Houston to come monitor my elections in Louisiana——

Mr. ROHRABACHER. All right.

Mr. SCHEDLER. —and I would suggest to you if I allowed that, I'd be run out of office in Louisiana, but especially——

Mr. ROHRABACHER. Well, the——

Mr. SCHEDLER. —with the conversation we're having. But I know of zero.

Mr. ROHRABACHER. Does anyone disagree with that on the panel? Yes, sir.

Dr. WALLACH. So the nature of the threat is that they don't want you to see them there, so we can't assume that if we haven't seen them, that they're absent. What we do know is that we've established motive. The attack on the DNC's email server is motive for a nation—it shows that they did it for explicitly partisan purposes. And when you combine motive with means and opportunity——

Mr. ROHRABACHER. Excuse me. What example was that that you just gave?

Dr. WALLACH. Oh, I'm sorry. This was reported in the press that Russian state actors allegedly hacked the DNC's email server with the intent of releasing emails for partisan purposes.

Mr. ROHRABACHER. Okay. But that's not the election process, but that is an entity that's involved in elections here so they have capability of actually getting into various—whether it's Republican, Democrat, or whatever, but actually in the election process we have no examples of them actually hacking into the system and compromising the integrity of any specific election, is that correct?

Dr. WALLACH. The only example I'm aware of happened in the Ukraine in 2014.

Mr. ROHRABACHER. Right. Okay.Just to let you know, we have seen article after article after article about how Russia is compromising the integrity of our election system. And, Mr. Chairman, the panelist is just saying that is false and just a note.

For those of us who want our country to be safe but we also don't want to just continually vilifying Russia turning them into the bad guys. If we're going to have the integrity of our system, I think we have to look at home for some of the real threats to the integrity of our voting system and whether the—as we say, the old-fashioned way of stealing elections has been around for a long time and we should be insisting that we make sure that we don't have people, for example, voting who are not eligible to vote because they're perhaps not citizens or here illegally.

We have people who are trying to suggest that we don't even have any real demand to identify someone's self whether they are here—whether they are actually who they say they are when they go to vote.

So we have a real challenge to make sure our system is, as I say, safe from being defrauded because the people of the United States, their ballots are being negated by every other ballot that's cast is cast by someone who does not have a right to vote here.

Now, with that said, we actually did confront this. Congress confronted this whole issue back in 2002 with the Help America Vote Act. And just very quickly to the panel because my time is running out, that's been around now since 2002. Congress passed this act specifically aiming at protecting the integrity of our system. Is our system now more or less at risk from cyber attacks due to this legislation? And very quickly, if we could have the panel answer that.

Dr. ROMINE. I think the legislation has improved our focus on security issues associated with the voting system. My organization has been working in partnership with the Election Assistance Commission under HAVA for 14 years to provide the best guidance possible to States and municipalities.

Mr. SCHEDLER. I would certainly echo that comment. And if you allow me just to claw back on you previous comment, I mean the whole Russian argument has—they've actually accomplished I think—even if they're not trying, we've done it for them, quite frankly.

Mr. BECKER. Yes, I agree. I think the Help America Vote Act has helped improve security since it was enacted, but even more importantly, what we've learned since it has been enacted has helped improve the security. I think the 2016 election is going to be one of the most secure we've seen in recent memory but there's no ques-

tion that I think based on what we're talking about here and this discussion and the conversations we're having, the 2018 and 2020 elections will be even more secure.

Dr. WALLACH. So HAVA helped us get rid of punch cards and helped us get rid of lever voting machines, and that's a good thing. HAVA was really two parts. It helped create the EAC, which could then help improve standards, and it also helped fund the purchase of new equipment. The equipment was largely purchased before the EAC standards effort was in action, and I think it would be an excellent thing to revisit to get new equipment up to new standards.

Mr. ROHRABACHER. All right. Well, thank you very much and thank you, Mr. Chairman.

Chairman SMITH. Thank you, Mr. Rohrabacher.

The gentlewoman from California, Ms. Lofgren, is recognized.

Ms. LOFGREN. Thank you, Mr. Chairman.

It was interesting to listen to my colleague from California inquire about the role of the Russians in this election. And, I think, you know, the focus of this hearing is on the voting systems, but really the question is about the election and it's not limited to voting systems. And it's pretty clear that the Russians have attacked—have engaged in a cyber attack on the DNC and the DCCC. We've received reports on that. I thought it was unfortunate that the Republican candidate for President either thought it was a good idea or was making a joke about it—we don't know which. But this is a serious matter.

What we've been told is not just that the material has been taken but that the pattern of the Russians is not just to release material but to forge material and to alter it in an effort to try and impact outcomes of elections. And that's certainly—they have a history of cyber attacks in an attempt to discredit Democratic elections in Ukraine, in Bulgaria, Romania, the Philippines. So this is something I think we need to take very seriously. To my knowledge, this is the first time the Russians have actually so boldly attacked a Western democracy, in fact the most important democracy in the world.

Now, I think the focus of this hearing is unduly limited, and I agree that a large-scale attack on distributed voting precincts is unlikely to succeed, although I do think we've underestimated the potential impact of air-gap tabulation systems, and I think that is something to be concerned about.

But the question isn't really whether the actual vote tabulations could be altered because I don't think that's very likely, but whether chaos could be induced into the system. That is the goal of the attack on the Democratic Party, and I think it may also be the goal of the cyber attacks on the state systems.

What could be done with this voter information? Obviously, there are backups on the database so no one can alter who can actually vote. But what would happen if emails were sent to all of those voters or are just the Democratic voters telling them the date of the election had been changed or their precinct had been changed? Wouldn't that create chaos in a system if even a small percentage of those voters believed an email misadvising them?

I do think that there's a vulnerability in the overseas in system. The House Administration Committee has the primary jurisdiction

over election systems, and I remember we had a hearing talking about our lack of concern, the lack of concern that electoral systems professionals had about emailing the ballot to overseas voters provided that the ballot itself was mailed in. The more we think about it, with these hackings, if you altered the ballot on the email, you would again create chaos in the electoral system.

So I think that's really the goal here is not necessarily to impact the tabulation, although there may be efforts to do it, but to create long lines if people go to the wrong places to create chaos and to attack the faith and the confidence that the American people have in their elections systems through long lines and all sorts of mischief.

I do think that to downplay the role that the Russians have had in this is a huge mistake when you take a look at what they did to the DNC and the DCCC. And I'll just close with this. I do think that it's been disappointing. The reaction has been disappointing that if you attack one of the major political parties, somehow that's okay if it could be to your advantage.

I like to think if the Russians had attacked the Republican National Committee the Democrats would be as outraged as Republicans because it's an attack on America. It's not an attack on a party. And the fact that there hasn't been outrage expressed at all levels of both parties about the effort of the Russians to disrupt this election is—it's sad commentary on leaders of that party and it also is very chilling when you think about what could happen come this November.

And I see that my time is expired. I yield back, Mr. Chairman.

Chairman SMITH. Thank you, Ms. Lofgren.

And the gentleman from Louisiana, Mr. Abraham, is recognized for his questions.

Mr. ABRAHAM. Thank you, Mr. Chairman. And we'll get back on track here.

Secretary Schedler, let's go to the 30,000 foot view. In your opinion is the integrity and the security of the voting systems in all States—you being the past President of the Secretaries of State, you have I think some knowledge of the subject. You think it's good, bad, average?

Mr. SCHEDLER. Congressman, I would say it's good. I mean, we did a survey before this hearing and we got a response from, I think, 19 of 20 States to try to ascertain that. Aside from my knowledge from serving, and I don't profess to be an expert on every state system, but there's a lot of similarities, there's a lot of differences in the States and that's what makes it so unique. But I feel very comfortable again—and the representative from California who appears stepped out.

Keep in mind the Democratic National Convention, the component that was hacked was the campaign side of it. Each and every one of us like me is elected. All of you have used a campaign commercial list to determine a mail issue, a walk list in a neighborhood, whatever it may be. Those are readily accessible. I'd sell you mine. If you know me well enough, I might give it to you.

But that is vastly different than the registration component and certainly vastly different than the Election Day component of equipment. So I think you have to understand that forefront to get

into this subject. There's no one minimizing what happened with the Democratic National Convention. I know I have and I know with one of my colleagues, and that makes no difference if you're in a red state, blue state, or purple state.

But the bottom line is maybe it's just our knowledge of the system that gives us this feeling of somewhat—not overconfidence because I think this is a good thing that we're going through, but we all remember the year 2000 when the world was going to end at one second after midnight. I'm still using batteries my wife bought for that event. That does not mean that we did not have reason to believe with studies and we should have been prepared. We went through that gyration. Or when a ballgame—when the scoreboard goes out on a football game, if you're sitting in the stands, you know what's going on. And guess what? There's other people taking track of those statistics at that same time.

It's the same with election systems. If one component goes down, we have various components that come in and—it may delay it some but it doesn't create a nuclear war.

And I can't speak to what happens in the Ukraine. I can only speak to what happens in the United States, and I'll tell you, the election system in the United States, just like many other things in this country, in spite of maybe what we think, is the best system in the world. Is it fool-proof? Absolutely not.

And I'd also tell you there's no such thing as a perfect election. Anybody that tells you that don't know what they're talking about because anytime you've got 10,000 machines at play and 15,000 people from 65 to 90 years old, things are going to happen. It's how you handle that. It's how you document that and move forward.

So I'm very confident in it with caution lights on. And there's no disrespect to anyone who believes otherwise. We're looking at it. It's forced us to do so. But I am deeply concerned, and I can speak to my Democratic colleagues and my Republican colleagues that have been on conference calls over the last several weeks with this issue. We are in unison. This is the worst situation we could be talking about as we enter this election. We've been going through a chaotic convention process. We have voters who are more disgruntled than ever. And we are adding to that participation rate in a very negative fashion.

And I feel very comforted in saying that I speak for all of my colleagues that we are deeply concerned with the rhetoric that's going on right now from the national press, and we're not trying to minimize it. We're double-checking, but there's little that could be done in eight weeks, little. We just need to stay the course, have confidence in what we're doing. And again, I'm very confident that on November 9, you're going to wake up and you're going to have unofficial result of who won the President of the United States because keep in mind it's unofficial. We go through that audit in every county, every parish, every State postelection before it becomes official and you go to your electoral college.

Mr. ABRAHAM. Thank you.

Mr. SCHEDLER. Thank you.

Mr. ABRAHAM. I'm out of time, Mr. Chairman. Thank you.

Chairman SMITH. Thank you, Mr. Abraham.

And the gentlewoman from Oregon, Ms. Bonamici, is recognized for her questions.

Ms. BONAMICI. Thank you very much, Mr. Chairman. Thank you all for your testimony.

Mr. Becker, you said in your testimony you emphasize that voters should feel confident in our voting system, and we certainly have heard a lot of messages about the importance of that confidence here today and how it will lead to greater participation, and certainly that's good for democracy. I think just getting the information out to the public that the voting machines themselves are not connected to the Internet is going to help. I think there's a misconception about that.

Well, I'm from Oregon, and we all vote by mail in Oregon. We've done that for more than a decade. It's a very secure process. It also makes it very easy for Oregonians to vote. The Secretary of State's office mails paper ballots to each and every registered voter a couple of weeks before the election, along with a voter's pamphlet with all the information about the candidates and the initiatives on the ballot so Oregonians have plenty of time to not only study the issues but then fill out their ballots and get them back in to be tallied by the local election offices.

And there are privacy and security measures at each step of the way. I was a trained election observer years ago and it gave me a lot of confidence to see each step of the way and to watch that tally happen at the elections office.

So I wanted to ask you a little bit about are there lessons to be learned from a State like Oregon that does use vote by mail with a paper ballot for everyone and really with a focus on the two different issues, there's the voter records and then there are actually what happens at the—with the ballot and the tally, the voting machine, if you want to talk a little bit about the lessons that can be learned from that system.

And then I also want to ask, Dr. Romine, I know NIST has mostly concentrated its work to date in standards development for the actual voting machines, but you're now, I understand, working to identify systems dealing with the voter registration systems. So—and just before you respond, both of you—I know Dr. Wallach mentioned something about the possibility of this selective disenfranchising of voters by deleting them from the database. It's really easy in Oregon for anybody to check whether they're still in the database, and getting the ballot early means that there would be an early notice that, well, maybe there was a problem assuming that somebody did get through a very secure system.

So, Mr. Becker, do you want to start and then Dr. Romine?

Mr. BECKER. Sure. Thank you. The—you know, of course Oregon and Washington have had long-time success with mail balloting in their States, and there are lessons that other States are learning from that. Not every State is the same, and other States have reached different decisions about their population of that, and that's entirely appropriate.

But States like California and Arizona and some other Western States offer the option of becoming a permanent mail voter, which you have to check a box, but after that you'll receive a ballot for every election. And I think very interestingly, Colorado has experi-

mented with a model—actually has put a model in place that—California just passed a similar bill that is a hybrid of sorts where every voter gets a mail ballot, but they can choose to mail that ballot in, drop that ballot off at a drop site, go in for early voting at a vote center as Dr. Wallach mentioned, which is they can go to any one within the county or they can even go on Election Day to a vote center and vote anywhere within the county. And they've seen some pretty strong initial successes there. So I think we're——

Ms. BONAMICI. But just to—I don't mean to interrupt, but just to clarify, in Oregon if somebody wants to go vote at elections—at the elections office on elections day, they can do that. They can stand in the booth there and vote. Anybody can do that.

Mr. BECKER. Absolutely.

Ms. BONAMICI. Most people don't because it's much easier to mail it.

Mr. BECKER. Right, and I think like—I think the States are learning from that experience and are trying to figure out what's best for their State based upon the successes that Oregon and Washington and Colorado and other States have seen with their particular systems.

I think also, importantly, you brought up the note between the voter registration systems and the voting machines and tabulation devices themselves. And I think particularly with mail voting it's very important because the voter lists are the way to deliver a ballot to someone because that's the list that generates the mailing to the voters. Of course, in States where they don't get ballots it's not that voters don't receive something else. They're usually receiving a card that's a reminder.

To the question earlier about chaos, which I think is a very important question, I think there's been a lot of work, contingency plans put in place by States to avoid chaos just in the last 10 to 15 years. One thing that's true now is particularly for Presidential election it's going to be very hard to avoid information about when the election is and what's going on. In fact, I'm guessing a lot of people right now would like to get away from information about the election.

So whether it's the work that Facebook is doing pushing information out about it's Election Day, click here to find your polling place, whether it's the work Google is doing the same way, whether it's the work of many other tech partners and States are doing partnering with those entities to make sure that information gets out, that's all a great protective measure to ensure that if a voter does experience a problem or might—think they might experience a problem, they can in advance go and make sure that they're getting the right information.

Ms. BONAMICI. Thank you. And, Dr. Romine, if you could briefly tell us what NIST is doing with regard to the actual voting machines now.

Dr. ROMINE. I think your question involved the whole lifecycle now from registration all the way through guidelines for the voting systems. The voluntary voting system guidelines that we work in collaboration with the EAC on involve the voting systems themselves, but I think we have a decades-long history of security as a

management of risk exercise, and I think the States have taken that very seriously. Our interaction with the EAC and with election officials in the States suggests that they are managing risk to the voting systems and to the registration systems in a way that incorporates the best practices that NIST has been promoting for a number of years.

Ms. BONAMICI. Thank you. I see my time is expired. Thank you, Mr. Chairman.

Chairman SMITH. Thank you, Ms. Bonamici.

And the gentleman from Georgia, Mr. Loudermilk, is recognized for his questions.

Mr. LOUDERMILK. Thank you, Mr. Chairman, and thank all the witnesses for being here today, a very important issue.

And rightly, we should be concerned about the integrity of our election system because we're only as good as the integrity of the selection system. After spending 30 years in the IT business, this is something that is very important to me and an area that I do understand at least from the technological side.

Another area that I think we have to be very conscious of is the federal involvement because typically whatever we get involved with doesn't run as well as if a State is doing it themselves, so I want to be very conscious of whatever role the Federal Government plays is very limited to—especially in an authority stance.

But I do understand that we do have some things that we can do as far as setting recommended standards, but recently, the Secretary of Homeland Security has reported saying that DHS is considering whether the state electoral apparatus should be designated as critical infrastructure. Dr. Romine?

Dr. ROMINE. Romine.

Mr. LOUDERMILK. —Romine, is this appropriate that—in your opinion?

Dr. ROMINE. Well, that's a policy decision that's way above my pay grade so I don't have any input that I can provide you for that.

Mr. LOUDERMILK. Well, I mean, do you have any idea what the benefits or the disadvantages would be of declaring these as critical infrastructure?

Dr. ROMINE. I can't speak to that. I know that NIST provided a significant benefit in partnership with the private sector on the development of a cybersecurity framework for improving the cybersecurity of critical infrastructures that has received a lot of attention and a lot of accolades. But that's not limited to critical infrastructures. Any organization of any size in any sector is free to adopt that framework.

Mr. LOUDERMILK. So you are working with DHS to help the States understand the critical nature of their electoral systems or——

Dr. ROMINE. Absolutely. We're partnering with DHS and with the Department of Justice on trying to understand how we can ensure widest dissemination of best practices to the States and municipalities. And as was mentioned earlier, request to DHS for assistance is not predicated solely on whether you are designated as a critical infrastructure. That request can be made without that designation.

Mr. LOUDERMILK. This includes cyber hygiene?

Dr. ROMINE. My understanding is it includes request for DHS to do scanning of systems, for example, but only upon request.

Mr. LOUDERMILK. So that would be voluntary? It'd be like a stress test on their system?

Dr. ROMINE. It would be——

Mr. LOUDERMILK. Are we applying lessons learned from the Presidential Commission on Enhancing National Cybersecurity in making these recommendations for the States?

Dr. ROMINE. So the Presidential Commission on Cyber Security has not yet reached the stage of finalizing the recommendations, so those are not being incorporated in these guidelines. And I would put it sort of in the reverse in the sense that the commissioners are actually taking a look at best practices out in the field and discussions with the IT industry and with stakeholders around the country to try to develop the best possible recommendations for the benefit of this Administration and the next.

Mr. LOUDERMILK. So NIST's stance on this is to work within the framework of the Federal Government to come up with recommendations that the States may or may not implement and with flexibility to where they can be customized to the States' individual networks?

Dr. ROMINE. That is correct.

Mr. LOUDERMILK. Secretary Schedler——

Mr. SCHEDLER. Yes?

Mr. LOUDERMILK. —how do you feel about that?

Mr. SCHEDLER. Well, I do not think critical infrastructure is needed at all. I mean, as was indicated by Dr. Romine and I did a little bit earlier, we can go to Homeland Security now, we can get those tests by FBI. We have a committee—matter of fact, your Secretary of State Brian Kemp, who has been very active in this whole process with several of us, is one of the committee members that we've appointed from NIST to serve on the Homeland Security Committee and to do best practices and the like.

So most States are cooperating with their local FBI agents when needed, and you know, again, I don't mean to be flippant but do we really want to create a new TSA for elections in this country or a new Postal Service? I just don't think we need that. The Constitution says very vividly that it's up to the States for the time, place, and manner in which we conduct elections.

It is a constitutional issue, and I understand that from the rhetoric that's not the intent, but to go and put the national elections on par with the banking system and the electrical grid, in my point—in my position is way overreach, unnecessary, and we can accomplish the same goals. It's not that we don't want their support and assistance when we need it, but we can accomplish that in a far less intrusive way, I think, if we just keep things on pat now.

And again, I think the answer is part of new equipment, new HAVA dollars, whatever it may be to improve these systems. We're working on trying to get a system where you can vote anywhere in the State, just like was represented earlier.

So critical infrastructure would be an absolute—and I think I speak again for—I don't know of any Secretary of State that's voiced an opinion that they want to be part of that.

Mr. LOUDERMILK. Do you feel what NIST is doing is beneficial to you?

Mr. SCHEDLER. Yes.

Mr. LOUDERMILK. Do you feel in any way that what's happening right now is a camel nose under the tent?

Mr. SCHEDLER. No.

Mr. LOUDERMILK. Okay. All right. Thank you. I yield back, Mr. Chairman.

Chairman SMITH. Thank you, Mr. Loudermilk.

And the gentleman from New York, Mr. Tonko, is recognized.

Mr. TONKO. Thank you, Mr. Chair. And welcome to the panelists, and thank you for your information.

Mr. Becker, the 2014 Presidential Commission on Election Administration recommended that audits of voting equipment be conducted after each election as part of a comprehensive audit program. According to verified voting, approximately 3/4 of voters in November will be using voting machines with a paper record of their vote. And I'm—just share a concern perhaps about the potential for mishaps or potential hacking for the voting machines with no paper trail. Can you please describe the role auditability plays in elections and the impact individual voters casting their vote?

Mr. BECKER. Yes, thank you. So in—we—of course, auditability is important. If—it's very helpful when there is a permanent record created that should a count need to be reviewed for some reason—and in fact there's a process in place to discover even if you're not sure whether the count needs to be reviewed that you can discover that, and that's what a good postelection audit does.

In 2014, about 32 States offered—had a requirement for postelection audits. You know, I'll be honest. Some are better than others. There's very good standard practices where States pick random precincts across the State and check the paper count against the electronic count. There's even something called a risk-limiting audit where you escalate the number of ballots you have to count to ensure the result as the election gets closer, and these are practices that are put in place in many States.

What we are seeing is that it is easier to audit a system when you have a permanent record, a paper record that the voter has reviewed, and more voters are going to be voting on paper than we've seen since HAVA was enacted. States like Maryland and Florida, which had used paperless direct recording electronic devices, have switched. I believe this is actually—I'm a Maryland voter, but I—this is the first Presidential election since the passage of HAVA where Maryland will be using a paper ballot that's read via optical scan.

I've recommended for years—and States along with the Presidential Commission—that postelection audits are a good idea, and having a system that allows for full and transparent postelection audits and paper right now appears to be one of the best systems for that, affords the best opportunity to ensure that the election results are—do reflect the will of the people.

Mr. TONKO. Thank you. And, Secretary Schedler, would you please describe what you have in place in Louisiana in terms of postelection auditing, and how would you rate other States overall?

Mr. SCHEDLER. Well, we do have a post-audit function. Now, we do not have a paper ballot system after we are looking at that when we go out for RFP next year on a new system, but we do—of course, our screen under HAVA does—after you complete voting, it pops up and gives you everything of who you—every person you voted for, position you voted for. They give you one more opportunity to rectify that if you want to change it or there was an error.

What we see a lot on highly sensitive machines is an elderly person may be dragging their hand and it inadvertently hits the button below or a lady with long fingernails, sometimes it will have a problem, but you do have the opportunity to rectify that. But we do audit after every election. We audit at the end of each day on early voting to ascertain the correctness of the vote and basically balance the balance sheets so to speak so——

Mr. TONKO. Right. And so you—there are the paper ballots that you're devising an audit process for?

Mr. SCHEDLER. That is correct.

Mr. TONKO. What are some of those factors in that audit that you absolutely see essential? What—have you looked at other States and what they might be doing or——

Mr. SCHEDLER. Right. We've actually gone out to Denver. The county of Denver has a very similar situation that is now being used in California and other States with the paper ballot where the majority of folks actually want to bring that ballot in and put it into a box so to speak at a site. So we've looked at that system.

We've looked at the printing of a paper ballot instead of on the screen that would go into a locked box. I would be personally against that voter taking that ballot out of the precinct. I think there's one State that does that.

But overall, to answer your question, I mean I think the systems are sound, but everyone has to remember every State is different, and that—I think that's the uniqueness of the system, a lot of similarities, but each State is very unique in the way they do their elections. Some may have a week of early voting, some may have 30 days. Some States have no early voting, and that is the prerogative of that State.

Mr. TONKO. Thank you very much. Mr. Chair, I yield back.

Chairman SMITH. Thank you, Mr. Tonko.

Mr. Davidson is recognized.

Mr. DAVIDSON. Thank you, Mr. Chairman.

Dr. Wallach, your testimony addresses the possibility of inserting malware into voting machines themselves. Can you elaborate on how malware could be loaded onto machines that are not connected to the Internet and further explain what it means that each and every single voting machine has to be manipulated? Or is there a different way where you could just hack one machine and that would transmit a bug to other machines in the precinct, again, even though they're not connected to an Internet?

Dr. WALLACH. Sure. So before we had an Internet, we had computers with floppy drives and there were computer viruses that could spread from one computer to another over floppies. Electronic voting machines, some of them use memory cards, some of them have these big battery packs, some of them have local area networks.

Studies conducted in 2007 by the State of California State of Ohio, State of Florida found security vulnerabilities that could take advantage of these to engineer viruses where one compromised voting machine could then infect eventually the entire fleet of machines for an entire county.

Mr. DAVIDSON. Okay. So, you know, it's accurate to say that just because something is not connected to the Internet, it does not have vulnerability to cyber attack?

Dr. WALLACH. Being disconnected from the Internet helps, but it's not a panacea.

Mr. DAVIDSON. Okay. Perhaps as Secretary of State, Mr. Schedler, you could talk about—I spoke with our Secretary of State Husted about their protocols, but perhaps you could elaborate on how do your procedures protect against that risk should something like that occur?

Mr. SCHEDLER. Well, I think it's important to remember that, you know, we never link machines together. I know that some new systems that are being touted like a Wi-Fi and if you had a multiple-precinct site where you have a Wi-Fi, now that to me is a little scary.

But when you consider the concept of each individual machine has a cartridge that's delivered by my office—now, we're a top-down system. We're not by county in Louisiana so we are vastly different. But—two or three days before, we literally deliver all the cartridges for all 10,000 machines to the various parishes, counties, to the clerk of court. The morning of the election—and we—when we deliver a secure laptop that is our equipment, it's not used to go shop on Amazon or anything else.

And the morning of the election the commissioner in charge for that precinct picks up those cartridges and puts that cartridge individually into the machine, turns the machine on, and at the end of the night that cartridge is retrieved. It is driven back to the clerk of court with a sheriff's escort usually, and it's imported into that laptop. And it is on a closed-circuit line sent to my office in Baton Rouge.

Mr. DAVIDSON. Okay.

Mr. SCHEDLER. So, I mean, it is a little bit different, but to my knowledge no State interlocks machines so the concept of getting into one machine with one cartridge and you miraculously change all 10,000 across the State is ridiculous because you'd have to go into each machine individually and you'd have to have the programming.

Mr. DAVIDSON. Right. So in your system you have one card. Ohio system is similar. You have one card goes to one machine.

Dr. Wallach, you mentioned a case study in Ohio. Perhaps you could elaborate on what that real vulnerability is.

Dr. WALLACH. Right, so the study in Ohio was called Everest, I believe. The similar study in California was called the Top-to-Bottom Review. I was part of the Top-to-Bottom Review. And each of these studies found ways that regular poll workers and election officials going through their standard procedures and standard operations could unwittingly be used to transmit viruses from one machine to another through the motion—typically, at the end of the Election Day you move a memory card through each of the ma-

chines in the precinct, and that's to collect the vote totals. That process can spread a virus. And there are other processes. The details vary from machine to machine.

Mr. DAVIDSON. Would a centralized federally controlled national voting infrastructure increase or decrease that risk?

Dr. WALLACH. That depends how it was built. I've been working with Travis County on trying to design something new where this wouldn't be a problem. The system that Los Angeles County is working on, this wouldn't be a problem. The reason why is because they generate paper backups—or rather paper ballots, which could then be audited against any electronic results.

Mr. DAVIDSON. The machine itself has memory, the card has memory, and it prints a roll tape that stays secure inside the machine and you can audit any one of those, so it's a good system in Ohio. It's been tested a lot. And Ohio will likely be front and center again in this election.

Dr. Romine——

Dr. ROMINE. Romine.

Mr. DAVIDSON. Romine, sorry. You stated in your written testimony that the NIST voting programs partnered with the AC to develop the science tools and standards necessary to improve accuracy, reliability, and usability and security of voting equipment used in federal elections for both domestic and overseas voters. How do you measure these improvements? How do you quantify them? Are there qualitative, quantitative measures?

Dr. ROMINE. There are both. I don't have the details today on exactly the measurement of those improvements. I'd be happy to provide those to you. I think the issue, to a large extent, has been listening to the accessibility community. The human factors research that we've been able to do demonstrates certain kinds of changes that can be made to improve the accessibility and the usability of electronic voting systems, and we've documented those in various reports. I can give you pointers to those reports for the way in which those systems have been improved.

Mr. DAVIDSON. Okay. Aside from identity theft—my apologies. My time is expired.

Chairman SMITH. Thank you, Mr. Davidson.

And the gentlewoman from Maryland, Ms. Edwards, is recognized.

Ms. EDWARDS. Thank you, Mr. Chairman. And thank you to the witnesses. I apologize I had to step out for a bit, but I came back because this is a really important subject to me.

I just want to be clear—and a yes or no answer from each of the witnesses would really help. Is it your—do you concur in the belief from the Department of Homeland Security that it was Russian state actors who hacked into both the Illinois—or attempted Arizona and also the party hacking that occurred earlier in the year? Dr. Romine?

Dr. ROMINE. I have no information on that other than what's in the press.

Ms. EDWARDS. Secretary Schedler?

Mr. SCHEDLER. Well, I mean the only thing I know of the Russian is the DNC issue. I don't know if they've ever determined where it came from in Arizona or Illinois.

Ms. EDWARDS. Thank you. Mr. Becker?

Mr. BECKER. Yes, I don't have any specific information. I'll defer to the national security professionals on that.

Ms. EDWARDS. And you believe they're capable of making that determination based on the signature or whatever?

Mr. BECKER. I can't answer that without knowing the information they have. I don't have any information to the contrary to support it.

Ms. EDWARDS. Thank you. Dr. Wallach?

Dr. WALLACH. I only know what I've read in the press.

Ms. EDWARDS. Thank you. And, Dr. Romine, in fiscal year 2016, NIST received about $1.5 million in appropriations from the EAC. That is down from your budget of, I think, about $2–3 million in the previous couple of fiscal years. Do you think that that's sufficient for you to be able to provide the kinds of certifications that you need of election systems?

Dr. ROMINE. So let me clarify by saying NIST doesn't do certifications of systems. We do provide support through the development of guidelines in partnership with the EAC, and we also provide assistance to the EAC in the voluntary laboratory accreditation program the testing laboratories that do test equipment for certain—some States who choose to do that.

Obviously, the—you know, the truism you can do more with more, but we believe that the current budget that we're receiving is adequate for us to continue to provide expert advice in security and interoperability for voting systems.

Ms. EDWARDS. Thank you. And, Mr. Becker, in—you—in part of your testimony you indicated that the—I think it was your testimony that the technologies that we're using for these voting systems is now about a decade old for an awful lot of these systems. Can you share with us what you believe, if you've analyzed it, what would need to be an updated version of HAVA that would enable us to keep—to really keep track with the technology developments?

Mr. BECKER. Yes, and I think that might have been Dr. Wallach who said—who made one of those points. The—of course the—there is a rash of bought purchasing new equipment right after HAVA passed with a funding model that came through as a result of that. We've already seen some States like our State of Maryland and like Florida go to a second system after using the HAVA dollars.

I think in talking with the States there is a great desire to be able to leverage new technologies that will improve access, as well as the integrity of the systems, that will also be cheaper to maintain and that—I don't have a specific dollar figure. If we were to replace all these systems nationwide, it's definitely in the billions.

But, you know, to build—to encourage systems that are more component-based that use more off-the-shelf components that are easier to swap in and out so that you don't have a system that has a 10-year-old touch screen that you can update the touch screen as—with just the touch screen as it happens, I think that be a huge advantage to election officials. And if they had resources to do that, I think you'd find them doing some really exciting things.

Ms. EDWARDS. And, Dr. Wallach, because—I apologize. That was your testimony.

Dr. WALLACH. Sorry. No problem. Part of what—so I've been working with Travis County for four years now on trying to design a better voting machine, and very much our intent is to use off-the-shelf hardware with custom software to the extent that we can for exactly that reason. When you buy a giant touch screen computer from Hewlett-Packard, Dell, insert your favorite tech company, you can get cheaper warranty support, you can replace the machines whenever you need to, and that helps reduce your maintenance and ongoing support costs.

Ms. EDWARDS. Doesn't it increase your vulnerability though?

Dr. WALLACH. Not necessarily. The design of these systems, first and foremost, produces a printed paper ballot. So no matter what goes wrong with the computer, you have these printed paper ballots that the voters can see and verify. And everything else on top of that is gravy.

Ms. EDWARDS. Thanks. And then just as a conclusion, I want to thank Secretary Schedler because I think in your testimony you indicated that the Secretaries of State across the country have great confidence in this election, and I think that's an important message to convey to voters so that we can make sure that we don't, with all of this talk, depress voter turnout. And so thank you very much for your remarks.

Mr. SCHEDLER. Yes, ma'am. I appreciate that. And I know I speak for all of them. We're very concerned about the rhetoric at this time.

And if I could just add on the cost issue, I do have just on Louisiana, currently, we have roughly 10,000 voting machines that cost roughly or did cost $5,200 each on under HAVA so that—to replace those by today's dollars, if you could get the machine—which you can't—$152 million.

If we went to a system similar to what Mr. Becker just indicated to you—and I'm overly simplifying an iPad concept, whether it be proprietary or store-bought, less than $300 each. Now, you do need two to three per machine so the hardware costs for us in Louisiana, $152 million on the replacement if you could get it, roughly $50–60 million, 1/3 of the cost. And 75 percent of it is in the programming cost. The hardware is only 10 or $11 million.

Chairman SMITH. Thank you, Ms. Edwards.

The gentleman from Illinois, Mr. LaHood, is recognized.

Mr. LAHOOD. Thank you, Mr. Chairman. I want to thank the witnesses for being here today.

In my State of Illinois we've had a lot of changes in the last several years. We now have same-day voting registration, 40 days of early voting, extended grace periods, absentee voting has a lengthy period of time. And couple that with some of the issues we've had particularly in Chicago over the years with issues related to voting there, I guess in terms of educating poll workers or training poll workers or election judges and looking at methods, particularly as it relates to the integrity of voting on Election Day and as we look at potential hacking of machines, I mean, is there a good model out there that has worked in terms of how we educate folks that are there at the polls?

I'll also mention in a prior life I was Assistant State's Attorney in Cook County in Chicago. On Election Day, we would go out as

prosecutors and be there at the voting booth. And a lot of times we didn't know what we're looking for or what we were supposed to be doing.

And I guess, Secretary Schedler, can you maybe shed a little light on examples of what we need to be doing in terms of educating and working with our folks that are at the polls on Election Day?

Mr. SCHEDLER. Well, training is paramount. That came out in the Presidential Commission to all Commissioners or poll workers, whatever you want to refer to them as. We do a strong education component at the clerk's level. We assist with that. We have a very unified videotape that we use so we have consistency across the State. But we do heavy training and certification, and we require them to get certified annually. I think that's a huge benefit because the better trained, the better experience you're going to have on voting day.

We also use people in voting lines, especially at larger precincts for questions or promoting that GeauxVote app where you could let individuals take a look at a mock ballot and actually mock vote that ballot on that phone to use as a guide to shorten lines and have a better experience in the voting booth.

And the other thing that to me is a strength of poll workers and your voting boards in counties in regards to the subject we're talking about today, we all know our poll workers. They've been there a long time in most cases, great Americans. They do it for love of country, love of the experience. They don't do it for the money, that's for sure. And if you could just think about the greatest deterrent is that both Democratic, Republican poll workers together, do you realize if someone was going to affect an election, they'd have to go against that 80-year-old lady that's been there 30 years? I don't think that's going to happen whether they're Democrat or Republican.

And to me that's one of the hidden jewels in our system, whether you have the best state-of-the-art equipment or whatever we have, you've got people on the ground with two eyes and they're looking at the process. They know the process. And to me that's the strength of the American system at its core. And it's really fundamental. It's the same way we did it 240 years ago. And I just think that that's something that we need to recognize in this whole debate.

Mr. LAHOOD. And just as a follow up on that, the level of what you go through in Louisiana, are you confident that that type of education and training is consistent across the country?

Mr. SCHEDLER. That I couldn't speak to. I think it's dominant across the country, but I wouldn't say every State does it that way.

Mr. LAHOOD. And, Dr. Wallach, with all these changes we've seen recently with voting and how we vote—and I went to the litany there—what is the future of voting look like?

Dr. WALLACH. Well, I think what we've learned today is all the 50 States will be voting differently, and it's hard to make a broad-brush statement. I think that there will be a lot of hand-marked paper ballots scanned by machines. There will be a lot of computer-assistive technologies available, and there will be some States that are voting by mail and that's okay.

Mr. LAHOOD. Thank you, Mr. Chairman.

Mr. BABIN. [Presiding] Thank you.

I now recognize the gentleman from Virginia, Mr. Beyer.

Mr. BEYER. Thank you, Mr. Chairman.

Mr. Becker, I think in your comments you stated and wrote that there are 20 States in this Electronic Registration Information Center that you helped found. Why not 30? And then how do we motivate the other 30 to be part of it? And is there any suggestion that we'd ever require that?

Mr. BECKER. I feel like I planted that question with you, and just for the record I—we've never talked about this before.

So the Electronic Registration Information Center, ERIC, is a data center that States voluntarily choose to join, and they share information so that they can identify when a voter record is out of date so they can notify that voter, make sure that voter gets the right information at their new address and also reach out to all the people who are eligible to vote but aren't yet registered and direct them to the easiest way to register. It was founded in 2012 with just seven States, so it's only four years old, and now 20 States plus DC. are in it so I think that's pretty good for a—you know pre-K 4-year-old.

But certainly, you know, we are working very hard with the States that are already in it, including Virginia, who was one of the founding members, to see more States join. And as the word gets out, States like Virginia and Louisiana and many other States are spreading the word that this is helping them keep their voter rolls up to date and, in turn, what that's doing is actually reducing costs and increasing integrity because they're not sending mail out to people who no longer are there.

The Presidential Commission on Election Administration, of course, did recommend that States join systems like ERIC, and that has been a tremendously positive influence. And I think by the time we get to the 2020 election I think we will be at more than 30 States, as I've talked to other States around the country.

Mr. BEYER. Great. A parallel question for Dr. Wallach. In Mr. Becker's testimony, he talked about how the postelection audit requirement that mandates States match paper to digital is only 32 States doing this right now. And you wrote the mere possibility of a recount or audit of the paper ballots acts as a deterrent, dot, dot, dot. So what do we need to do with the other 18 States that don't have this post-audit reconciliation of paper and electronic?

Mr. WALLACH. Well, I'm certainly a big fan of reconciling paper and electronic records when you have both. Many of the States, that's not an option because you don't have paper records like, for example, the entire State of Georgia votes entirely on electronic machines without any paper records. So there's no way to do a meaningful audit. I would love to see the sun-setting of those machines and replacing them with the next generation of machines that will have paper.

Mr. BEYER. There was the mention that we have $396 million of authorized but un-appropriated HAVA money. Is that enough to replace the old machines, the bad machines?

Dr. WALLACH. I'm not sure. If we could do it on a shoestring or if we'd do better to spend more money and do it properly. I don't have a good answer for you today.

Mr. BEYER. Thanks. Many of you wrote about how the machines aren't connected to the Internet. So, Secretary Schedler, if they're not connected to the Internet yet, Dr. Wallach pointed out that they are at the time of initialization and tabulation. I think someone else pointed out that they're usually connected to the voter databases, you know, 365 days a year. So how—is that actually a strength that we can talk about that we're not connected to the Internet, or are those holes at initialization and tabulation——

Mr. SCHEDLER. I would think it's a strength because, as I look to the—I mean, people—the most common question asked of me is, Secretary Schedler, when are we going to be able to vote on the Internet? And my answer is I hope never because the world is evolving and we see it. I mean, the Department of Defense gets hacked into. Everything gets hacked into. And that's why I'm so adamantly—I want to keep it with the States to decentralize it, make it much more difficult. But the day we go on the Internet, all bets are off as far as in elections.

Now, I want to caveat the comments. There are a couple of States that do allow a return of an overseas military ballot via the Internet. I think four, I believe, Alaska being one and I don't know—remember the other three. So I want to clarify that. Now, that's a small percentage of the overall vote. But they do allow a return of—but I will say this in defense of that, although we don't do it, it is a secure—you know, military—they have to get a pin, you've got to have access. You just don't just send them an email and here it is. They have to get access and have ability to open that file up and do something with it. So it is a little bit different. But certainly, under the argument and discussion we're having today, could be vulnerable.

Mr. BEYER. Great. Great. Thank you, Secretary.

Dr. Romine, a quick question. On this postelection audit requirement of reconciling paper and digital is—will—is this a NIST suggestion or a NIST standard or should it be?

Dr. ROMINE. Part of the voluntary voting system guidelines that we worked with in the EAC was a strong recommendation that there be an auditability or audit capability, and certainly paper records provide a really robust way to do that, but it doesn't mandate specifically paper records.

Mr. BEYER. Okay. Thank you very much. Mr. Chair, I yield back.

Mr. BABIN. Thank you.

I now recognize myself for five minutes.

Secretary Schedler.

Mr. SCHEDLER. Yes?

Mr. BABIN. By the way, I just spent two days in Baton Rouge, and my heart goes out to you——

Mr. SCHEDLER. I thank you for——

Mr. BABIN. —and your State.

Mr. SCHEDLER. —coming. I came back with Representative Honeycutt. I came to Washington yesterday with him——

Mr. BABIN. Right.

Mr. SCHEDLER. —with Garret Graves and Steve Scalise, flew with them, and he had the same expression to me so——

Mr. BABIN. Unbelievable. I represent the 36th District in Texas right across the Sabine so—and we had—in March we had——

Mr. SCHEDLER. Well, you all know shares of rain, too.

Mr. BABIN. Absolutely. But I've never seen anything like that.

Mr. SCHEDLER. No, it was pretty—30 inches of rain in some spots, 25, 30——

Mr. BABIN. Absolutely.

Mr. SCHEDLER. —inches of rain.

Mr. BABIN. In a population center like that.

But I'd like to ask you a question. You stated in your testimony that "I'm happy to report there's no evidence that ballot manipulation has ever occurred in the United States as a result of the cyber attack." And, Dr. Wallach on the other hand states that "If our paperless electronic voting systems were attacked, we'd be unlikely to see evidence of it in the voting machines or tally systems."

So I just want to hear both of your opinions on this matter. I'm not trying to start——

Mr. SCHEDLER. No, no, no.

Mr. BABIN. —any problem.

Mr. SCHEDLER. I know you're not trying to start a war——

Mr. BABIN. Yes.

Mr. SCHEDLER. —or anything. I'm a pretty simplistic kind of guy——

Mr. BABIN. Okay.

Mr. SCHEDLER. —you can see in my delivery. I asked a simple question and I do not profess to be an IT expert, but I come at the derivative of saying if you're not on the Internet with voting, how do you hack into the machines? And I'm just coming at it very simple——

Mr. BABIN. Yes.

Mr. SCHEDLER. —apple pie. I don't know much more than that, but if you're not on the Internet out in the cloud how do you hack it? If they're individual machines with cartridges——

Mr. BABIN. You bet. Thank you. Thank you. And, Mr.—Dr. Wallach?

Mr. SCHEDLER. If he gets deep on me, I'm not going to be able to argue with him.

Mr. BABIN. Thank you.

Dr. WALLACH. Right. The example that I think we can look to to understand this was the Stuxnet virus, which was apparently engineered to damage the Natanz nuclear refinement facility in Iran. That nuclear refinement facility was also meant to be secure. It also was not connected to the Internet, yet somehow this Stuxnet malware was able to do its job. We don't know many of the details, but it's quite clear that where there's a will—and presumably a budget—then there's a way.

I don't know whether our nation-state adversaries have chosen to make that investment, but I know that it's technically feasible to mount these sorts of attacks and that's why it's important to take mitigations and defensive steps against them.

Mr. BABIN. I agree with that. I sure do. Thank you. Thank you very much.

The next question would be for you, Dr. Wallach. Is it possible for someone to conduct a cyber attack in case of voting or election systems while pretending to be Russian, Chinese, North Korean hackers so as to falsely assign blame for the hack on a foreign nation? And have you ever come across any instance of such in your experience?

Mr. WALLACH. So the issue of attribution of cyber attacks, broadly speaking, is a well-known problem and nation-state actors will pretend to be other nation-state actors for exactly the purpose of trying to throw off attribution.

Mr. BABIN. Yes.

Dr. WALLACH. So I am not privy to however we have this Russian attribution. I have to assume that the people who said that know what they're doing.

Mr. BABIN. Okay. And then, Secretary Schedler, one more for you. Considering the range of vulnerabilities—and this follows up on what you said just a second ago—the range of vulnerabilities that exist for electronic systems, do you think that more States will eventually return to paper ballots? And if so, can you explain to us how paper is the more secure option?

Mr. SCHEDLER. Well, there seems to be a trend if you consider a trend what four States, five States now, but in many cases it's done for cost reasons also. I mean, you have to factor that in.

Mr. BABIN. Right.

Mr. SCHEDLER. I'll say this. You have to have some other protections, and I think Oregon and some of the others do, but I mean I've always said that the best way and easiest way to perfect fraud is right here in my hand.

Mr. BABIN. Yes.

Mr. SCHEDLER. You know, when I mail out a paper ballot, I have no earthly idea who actually votes that ballot. I may be able to verify a signature, but I can tell you that we've had a couple of cases in Louisiana on mail ballots with frail and elderly in a small jurisdiction where the individual canvassing the area goes to Ms. Suzy and Mr. Joe's house, knocks on the door, says, oh, can help you fill out your mail ballot? And they do. Need I tell you how they vote? We caught one guy. Instead of keeping the addresses of 15 elderly people, he sent it from his campaign headquarters.

But the point being, you have to have some checks and balances even under that system even if you're verifying the signature with electronic machine or signature, not naked eye. So I always contend that this right here is the easiest way to perfect fraud in the system. Now, it doesn't mean that it's wrong to do it because I'm very respectful of other States and how we do it.

But I will just say this. In the entire subject matter we had HAVA dollars ten years ago, and I think this will set the stage with sparse dollars in States and in this country at this time. We have $386 million of un-appropriated HAVA dollars purportedly still out there. I gave you an example of what are the costs to replace Louisiana systems. So $394 million may go a long way, if not completely retool all 50 States with assistance from the Federal Government.

But we can put layer on top of layer on top of layer of what ifs and what have you, and as long as you all can write the check,

we'll do it. But at some point you've got to use practicality here, and I am again—myself, and I think I speak for all 50 of us—we are very confident in the system we have. We have trifecta backups, audits and the like, and even under some of the worst-case scenarios that I've heard here today, I am still very confident that you may not have results November 9 if catastrophe hits, but if you're a little patient with us, we'll get you the results and you'll have a new President of the United States.

Mr. BABIN. That's a good answer. Thank you. And I know I'm out of time, but, Dr. Wallach, just as short as you can, what do you consider the chances with many States going back to the paper ballots?

Dr. WALLACH. Well, if for no other reason than electronic voting systems are very expensive, as the Secretary told us earlier——

Mr. BABIN. Right.

Dr. WALLACH. —and paper systems are cheaper, and for that reason, if nothing else, while these electronic systems are wearing out, we're moving to paper sort of by default.

Mr. BABIN. Okay. All right. Thank you.

Let's see. I recognize the gentleman from Illinois, Mr. Lipinski.

Mr. LIPINSKI. Thank you. And I thank all the witnesses for your testimony. And I have—I'm not sure if I can get to my questions because some other ideas came to mind as you're talking here. So let me ask a couple things here so I better understand. I know States—everyone does it differently, and the idea of not having our—the machines directly connected to the Internet makes sense.

But, for example, if you do have a voting machine, you're voting, usually then at the end of the day when the votes are—polls closed, votes are tabulated, how are those votes then communicated then from the polling place? So—because I would expect that they are done oftentimes over some sort of connection to the 'net.

And then the other part of that is I go online election night and I'm looking at the results coming in so I can go online and connect in at least to see the results that they're displaying. So hopefully, I'm not displaying too much lack of understanding here, but aren't there some connections there to the Internet that are going on?

Mr. SCHEDLER. Not—no. Each machine has a separate cartridge and it's independent. They're not—none of those machines are linked together. And to answer your question, what occurs at the end of that night is that cartridge is retrieved from that machine. It is taken to the clerk of court or the central location in that county—at least in the parish in Louisiana—and it is put into a secure laptop and transmitted on a closed-circuit line, not on the Internet.

Now, we do have—I mean, there's other systems. There's a tape on all machines that we can replicate. If a court challenge to an election—I can't tell you how you personally voted but I can certainly tell you if you voted and I can reconcile that tape. And there's one other method. Even in the transmission of those results on the nightly news that you referred to, there is a delay and there is a reason why we have that delay, to be able to detect any interference in that process.

And again, even it occurred, delaying in getting you official results—because keep in mind on election night the results are unofficial. We all know that from being elected. The news media is out

there declaring winners before the polls even close. That's their job. Our job is to make it accurate and effective.

Mr. LIPINSKI. Well, that's good to hear. Is this—is that the common way it's done everywhere?

Mr. SCHEDLER. Yes, sir, pretty much. That's—to my knowledge, it's the way everybody does it.

Mr. BECKER. Yes, I can't speak for every place, but in the places I know of, they actually physically transport the cartridges or the memory devices with the counts that occurred in the precinct to the county office, which is often a frustration for people who are looking for election results because if they hit traffic or something like that, there's going to be a delay in getting those results. And only at that point—and most of these devices or many of them at least have duplicate cartridges as well, so one of them will go to the central count to be incorporated and you can check them.

This is not completely foolproof and this—but it's—the problem that we often see is that voters get frustrated because there's a little bit of a delay in getting it because there's a physical transportation of the memory cartridges.

Mr. LIPINSKI. And I think that—hopefully, that helps alleviate a lot of concerns that people do have that you—it's not being transmitted electronically in the way that can be hacked into.

One other question that I had, the paper tapes I think are—certainly, I agree—a great idea. How often, though, and at what point would there be a check of those against the electronic numbers?

Mr. SCHEDLER. It usually dictates—I mean, it's usually dictatable by the closeness of the election. I mean, usually a challenge or if there was some major malfunction, but typically it's triggered by a challenge by a candidate, someone, you know, wins by 10 votes or loses by 10 votes, challenges that and requires a recount to be taken.

We are also very public with the certification of our machines or you as a candidate or a campaign can watch us certify those beforehand in the warehouse and also when we reopen those machines to recertify candidates are allowed to come in or representatives to actually watch that process and to watch all that matching go on.

I gave an—I testified last week at the EAC on this subject, and if you can bear with me a minute, it probably is a good representation of your question. I watched in utter awe with major networks with an individual that was claiming he had a handheld device that he could put early voting cards into and vote as many times as he wanted. Now, I don't argue the point that you can have a piece of machinery like that. They do it at gasoline pumps and the like. But what I did question was in the early stages they never, ever brought in anybody that ever conducted an election to dispute that.

And you have to allow for an early voting site that someone is going to sit there and watch as somebody keep injecting a card—how times are they going to vote? We have time limits in most States. But at the end of the day, even if you have that piece of equipment, you still have to have the programming of what engaged that card. And at the end of the day, if there were 100 people they came in to early vote by signature next to your name and we had 106 votes, we're going to be able to determine by that num-

ber on that card that you don't see of—that you voted six times. We don't know how you voted, but we know you voted six times so we'll catch you.

Mr. LIPINSKI. I am from Chicago, though.

Mr. SCHEDLER. I'm from Louisiana. We've got a lot in common. But we've cleaned that act up.

Mr. LIPINSKI. Similar.

Mr. SCHEDLER. We no longer throw ballot boxes in the Mississippi River. We don't do that anymore.

Mr. LIPINSKI. We have a big lake to do that.

Thank you very much. I yield back.

Mr. SCHEDLER. Thank you, sir.

Mr. BABIN. Yes, sir, thank you.

I now recognize the gentleman from Illinois, Mr. Hultgren.

Mr. HULTGREN. Thank you all for being here. This is such an important subject. I don't know if anything more important than making sure that our ability to vote is protected and that we feel confident that everything is being done to make it open and accessible to everybody and using technology to do that but at the same time making sure that we're protecting information and protecting that confidence that our voting booths are accurate and are being abused in any way. So I really do want to thank you for being her. Thank you for your work.

It's certainly clear the nature of our increasingly connected world has opened up new vulnerabilities which were originally unforeseen. It's also brought about new great things that we all can agree improve our lives, the functionality of our democracy, and it does it in ways in which we can exchange goods and services with each other as well.

A little over a year ago, I had a chance to visit Estonia with a group of my colleagues and saw many of the innovative ways they are integrating technology into their government services. They actually have online voting in many elections and most forms and bureaucratic paperwork are submitted online in more easily searchable formats.

While this is encouraging to me, I also realize that Estonia has as many people as New Hampshire or Maine, so there are things they can do differently than we as a country of almost 330 million people can do. So our States still need to have the flexibility to innovate and the Federal Government's role should be assisting but not passing down new unfunded mandates on them which we hear—I hear so often from my constituents and my local government officials and the challenges they face.

Dr. Wallach, if I could address my first question to you. Regarding the recent cyber attacks on the voter registration databases in my State Illinois and also in Arizona, why would an individual or an organization want to hack into States' voter registration information? Are they looking for the same kind of information other data breaches in the retail sector or just personal information or what's the purpose behind these attacks?

Dr. WALLACH. So there's a lot of different motives that we can ascribe. If we're talking about garden-variety, you know, identity theft, they just want to have the information in the database. If we're talking about the nation-state actors, their motive could be

to get information, but a lot of that information is available through other channels. It could be to tamper with information, and we've talked at length about the sort of chaos that you could potentially cause.

Mr. HULTGREN. Specifically with tampering, once a hacker has gained access to a database, would it be possible to add fictitious voters or delete legally registered voters?

Dr. WALLACH. If it's a database on a computer, it's possible to do all of those things.

Mr. HULTGREN. Yes. Okay. Dr. Romine, I wonder if I could address a couple questions to you. Is the walling off and protection of voter registration databases part of the technical guidelines for NIST?

Dr. ROMINE. The voluntary voting systems guidelines are principally for the voting systems themselves. However, we do have other guidance that my organization has developed over the years to protect information systems broadly, and this would fall under that category. And I think, yes, separation there is a legitimate way of trying to prevent certain kinds of interactions.

Mr. HULTGREN. So that separation is happening or is it——

Dr. ROMINE. What's actually happening in the States is something that I'm not privy to.

Mr. HULTGREN. Also, Dr. Romine, from what is known, what kind of guidance for protecting voter registration databases were in place in the two affected States that I mentioned earlier, Illinois and Arizona, and will NIST be considering updates to its technical guidelines to include voter registration databases?

Dr. ROMINE. I think we will be considering that with regard to our partnership with the EAC to provide guidance to the States and municipalities for protecting voting systems with a broader remit perhaps as one way to look at it. The guidelines that we have in place for IT systems have been developed over a number of years and involve integrity checks, identity management issues, and other things that can protect information and information systems. And so the cybersecurity framework that I alluded to earlier helps to—helps organizations to craft a way to manage risk in this space.

Mr. HULTGREN. Well, again, my time is almost up. Thank you for your work. Please let us know how we can be helpful going forward. And with that, I yield back to the Chairman. Thank you.

Mr. BABIN. Yes, sir. Thank you.

I now recognize the gentleman from Texas, Mr. Weber.

Mr. WEBER. I thank the gentleman.

I want to do something before we get into the election discussion today regarding the earlier comment from one of the members on the other side of the aisle that she was appalled that there was no Republican outrage over the Russians' apparent hacking of the DCCC. I would note that there's probably about the same amount of outrage from the Democrats over Hillary Clinton's dumping of a bunch of emails and destroying evidence in a federal investigation.

Having said that, in full disclosure I was an election clerk and election judge and a precinct chair for about 16 years in Texas in Brazoria County when we had good old-fashioned paper ballots. I was one of the few who raised my hand when they said, look, we

want to pass a resolution encouraging electronic voting. I said I don't. I like the paper system. I don't trust the Internet. That was back in the '90s. It seems as if we've come full circle now that you all are saying that there are some States who are literally considering going back to paper ballots.

So here's a question for, I guess, all of you one at a time. We'll start with you, Dr. Romine. Well, first of all, let's do it this way. How many States have paper?

Dr. ROMINE. I think there's only five States that are completely without paper. There are some States in the middle that have a mix, depending on the county, of paper and on paper systems.

Mr. WEBER. Okay. What States in your opinion has the best system, Dr. Romine?

Dr. ROMINE. I don't have insight into the systems that are being used State by State.

Mr. WEBER. So you really haven't formulated an opinion in that regard?

Dr. ROMINE. I don't have the data.

Mr. WEBER. Okay. Fair enough.

Now, if you say Louisiana, Secretary Schedler, I'm just saying.

Mr. SCHEDLER. My response to that would be the best system for which the people of that State feel comfortable in voting.

Mr. WEBER. Touche.

Mr. SCHEDLER. Okay. Because New Hampshire, I mean, if you can just think of the variety that we have across the board from the East Coast to the West Coast in Oregon, I mean, just totally different constituencies, totally different comfort zones, and, you know, if some people still like going to vote in their neighbor's garage and if that's what they want to do and then that's good for that State.

So, I mean, I guess that's the best answer I could give you. No, I wouldn't say that we're the best, although a few years ago Pew had us at number 18, which would surprise you I bet because I used to always say if you interview people on the streets of New York on the late-night television show, they'd never mention Louisiana in the top 20, but we're there. We've done a lot of——

Mr. WEBER. And they usually don't know what they're talking about anyway.

Mr. SCHEDLER. That's correct. That's correct. But I think that's probably—I know that's kind of a politically correct answer, but out of respect for all my colleagues and all the States, I think you have to make that decision.

Mr. WEBER. Okay. Mr. Becker?

Mr. BECKER. I'll also be diplomatic here. I think if you ask most election officials around the country at the state or local level, most of them will say that the technology they're using, none of them have found the ideal system yet, that they're looking for something new to come around.

Mr. WEBER. So you don't have an opinion about that?

Mr. BECKER. I don't have an opinion about a particular State. I think the work that's being done in places like Los Angeles County to come up with a system that's based on off-the-shelf components——

Mr. WEBER. Okay.

Mr. BECKER. —that is largely accessible is going to be very instructive to the entire field.

Mr. WEBER. Dr. Wallach?

Dr. WALLACH. Well, I'm going to toot the horn of three different States where I enjoy what they're doing.

Mr. WEBER. Okay.

Dr. WALLACH. I like California's use of risk-limiting audits where you can audit paper and compare it to electronic results. I like what Florida has done where they got rid of the paperless electronic voting machines. My parents live in Fort Lauderdale and they now vote on a laser printer will print out a ballot on demand so they can have early voting in vote centers. So Florida is now doing remarkably good stuff.

And, of course, I have to say something good about Texas. I think in Travis County we're building a really great system and it could potentially be applied in a lot of other places.

Mr. WEBER. Are you from Travis County?

Dr. WALLACH. No, I live in Houston. I grew up in Dallas.

Mr. WEBER. Okay. So let me just also say here, having been the recipient of—when a lot of those ballot boxes were carried—Brazoria County is a big area. Apparently, where I grew up is like 40 miles north of the county seat. And as an election judge, in the general election I was, of course, in the primary in the general election, too—we would always take our Democratic counterpart in the general election, take the ballot boxes down, turn them into the county. I've been on the receiving end of when it took, you know, 45 minutes to an hour just for the drive time and people were wanting those results.

One quick question because I'm the last one, is that right, Mr. Chairman?

Mr. BABIN. [No audible response.]

Mr. WEBER. Okay. What is the most critical time of a cyber attack?

Dr. WALLACH. I would say that a cyber actor who knows what they're doing is acting months to years in advance and—because they don't necessarily have access to——

Mr. WEBER. But I'm talking about if they were going to affect a November election coming up, is that something done the night of, the week before? You're saying years—are you saying they get into the system——

Dr. WALLACH. Yes. You get in way in advance and then you have whatever effect you're trying to have. If your goal is to create chaos, then you want to have your effect very late. It all depends what you're trying to do.

Mr. WEBER. Okay. All right, Mr. Chairman. I yield back. Thank you.

Mr. BABIN. Thank you. I appreciate that.

I want to thank the witnesses for their testimony and the members for your questions. And the record will remain open for two weeks for additional written comments and written questions from members.

And with that, this hearing is adjourned. Thank you.

[Whereupon, at 12:25 p.m., the Committee was 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

"Protecting the 2016 Elections from Cyber and Voting Machine Attacks"

Dr. Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology (NIST)

Questions submitted by Rep. Lamar Smith, Chairman

1. Going forward, what are the NIST research and analysis priorities for election security? Are these research priorities much different than NIST research priorities for cybersecurity in other areas?

   NIST Response:
   NIST is focused on research and developing guidelines to support the next version of the Voluntary Voting System Guidelines (VVSG). The scope of the next VVSG is under discussion with the Election Assistance Commission (EAC), the Technical Guidelines Development Committee (TGDC), election officials, and technical experts within the NIST/EAC Public Working Groups. At this time, NIST is working with the Public Working Groups to investigate security, usability, and accessibility considerations for a broader set of election activities and components, including voter registration, electronic pollbooks, blank ballot delivery, ballot marking, auditing, and election night reporting.

   NIST's work on voting system security has always been informed by the NIST cybersecurity program. Research in cybersecurity threats, technologies, and best practices provide a foundation for the security guidelines NIST develops within the VVSG.

2. NIST mandatory technical standards for federal agencies and voluntary guidelines for private businesses are available online. There is no intermediary agency like the EAC. Could NIST make its technical guidelines and advice available directly to the 50 states, without another agency playing an intermediary role?

   NIST Response:
   NIST works with many industries where NIST engages vendors and stakeholders directly. NIST's Smart Grid and Cloud Computing efforts are examples of this type of engagement. However, when NIST works on sector-specific guidance that falls under another agency's mission, such as voting and the EAC or healthcare and the Department of Health and Human Services (HHS), NIST collaborates with that other agency. In this instance, the roles of the EAC and NIST are set forth in the Help America Vote Act (HAVA).

3. NIST supplies technical guidelines for the Election Assistance Commission and the states to consider for protecting their voting products and systems against cyber-attacks. How are these election cybersecurity guidelines different from the cybersecurity guidelines NIST provides to federal agencies and private businesses?

NIST Response:
NIST's role under HAVA is to provide technical support to the EAC and the TGDC to support the development of the VVSG. The VVSG contains technical guidelines for voting system equipment in security, usability, accessibility, reliability and accuracy. The EAC's testing and certification program validates that voting systems meet these guidelines. The security sections of these guidelines cover a broad range of topics, including access control, cryptography, physical security, communications security, and auditing.

NIST's cybersecurity program provides the foundation for NIST's security guidelines for voting systems. NIST has an extensive set of general cybersecurity guidelines which are used by Federal agencies and voluntarily adopted by private industry to secure their information systems. These guidelines address technical, operational, and managerial security controls to help organizations better understand, manage, and reduce their cybersecurity risks. All of NIST's cybersecurity guidelines are freely available on the NIST website. State and local election officials can use all of these resources to secure their election systems. Some of these guidelines have been incorporated into the VVSG security requirements, such as technical guidelines on access control and cryptography.

While NIST's cybersecurity research in threats, technologies and best practices are broadly applicable to election systems, these systems have unique security considerations due to the specific security and privacy objectives for these systems, the technologies used in these systems, and the environment in which they are used. Guidelines for voting system security must take these unique considerations into account, while also ensuring that other important objectives can be met, including usability, accessibility, interoperability, and cost-effectiveness.

4. In your written testimony, you note how important it is to collaborate with all stakeholders in the realm of elections in order to be successful in creating voluntary standards. How often does NIST meet with election officials, industry, technical experts, and advocacy groups? What has been produced as a result of these meetings?

NIST Response:
NIST meets regularly with election officials, industry, technical experts, and advocacy groups through a variety of efforts. In the past several years, NIST has met with stakeholders through a number of venues, including large symposia, workshops, meetings, and on-going public working group meetings. In addition to regular interaction with election officials at the EAC Standards Board, EAC Board of Advisors, and National Association of State Election Directors (NASED) meetings, the following is a sampling of meetings, topics, and associated NIST outputs:

- Future of Voting Systems Symposia: NIST held two (2) symposia (2013, 2015) aimed at discussing the technology used in elections and identifying future needs for voting system guidelines. Over 500 participants including election officials, voting system manufacturers, test labs, standards developers, researchers, and advocates attended each symposium. Output from breakout sessions was captured by NIST and EAC leads and used to drive future discussions on VVSG scope and structure.

- National Association of State Election Directors (NASED) Subcommittee: NIST met several times in 2014 with the NASED Subcommittee, and representatives from the Bipartisan Policy Center and the Presidential Commission on Election Administration (PCEA). The NASED Subcommittee was tasked with determining a method for revising the VVSG in the absence of EAC Commissioners. In response to election officials desire to have a high-level set of principles as a replacement for the VVSG, NIST provided background information regarding the detailed requirements captured in the VVSG, the role of the voting system test laboratories (VSTLs), and EAC's role as a certification authority. NIST also prototyped a new approach, mapping NIST-developed high-level principles and guidelines, VVSG requirements, and NIST developed test assertions as a potential path forward for a new structure that meets the needs of all stakeholders, including election officials, manufacturers, and VSTLs. This approach has been further developed and agreed upon by NASED, the Standards Board, Board of Advisors, and the TGDC.

- Bipartisan Policy Center: NIST presented at the *Setting the Standards: What We Need From Our Voting System* meeting, sponsored by the Bipartisan Policy Committee and the PCEA. At this meeting, election officials, policymakers, advocates, and researchers explored the needed functionality in our nation's voting systems to conduct open, fair, and transparent elections.

- Roadmap for Usability and Accessibility of Elections[1]: NIST held two (2) workshops (2014, 2015) aimed at identifying current gaps and recommended solutions to ensure that voters can vote independently and privately. The roadmap was developed with input from advocates for people with disabilities, industry and academic researchers, developers, and election officials and presented for comment at the Future of Voting Symposium II (2015) and the TGDC informational meeting (July 2015).

- Usability of Electronic Pollbooks[2]: NIST engaged election officials and electronic pollbook vendors in analyzing the current landscape of electronic pollbooks and their use. NIST also developed analysis of e-pollbook usability, associated test plans and checklists, and presented information at NASED Winter Meeting (2015).

- Principles for Secure and Accessible Remote Ballot Marking Systems[3]: In 2015, NIST worked with usability, accessibility, security, and elections experts to define

[1] Roadmap for Usability and Accessibility of Elections, http://civicdesign.org/projects/roadmap/

[2] Usability of Electronic Pollbooks, http://civicdesign.org/projects/electronic-poll-books/

[3] Principles for Secure and Accessible Remote Ballot Marking, http://civicdesign.org/projects/remote-ballot-marking/

draft principles and guidelines for using remote ballot marking systems that support election integrity while ensuring that the system is accessible to all voters.

- NIST-EAC Public Working Group Meetings: The creation of the Public Working Groups was done as a direct response to feedback received from the PCEA, EAC Standards Board, and NASED. All of these groups made clear that the prior VVSG development process was inefficient and did not allow input throughout the process but instead solicited comment from the EAC Standards Board and non-TGDC members only after most of the work had been done. Additionally, the prior process did not take full advantage of the many election officials and other subject matter experts across the country willing to volunteer their time and offer their input during the development process. The Public Working Groups address all of those concerns by encouraging all interested individuals to get involved from the beginning through a transparent open process of development.

  NIST co-leads with the EAC the Public Working Groups and has engaged with the Election Working Group and provides technical leadership for the Interoperability, Human Factors, Cybersecurity, and Testing and Certification Working Groups. Together, there are 353 unique members from 20 state and 34 local governments, 11 manufacturers, three VSTLs, 12 universities, nine usability/accessibility organizations and five security organizations. The status and NIST outputs for each of the groups is given below. Many individual participants choose to belong to several groups, leading to aggregate participation numbers among all groups of 698 members.

  Election Working Groups: NIST engaged with the Election Working Groups and based on their definition of election functions, developed associated process models for pre-election[4], election[5], and post-election[6], all of which were presented for feedback by NIST at the EAC Standards Board, EAC Board of Advisors, and NASED meetings and used as input into the February 2016 TGDC meeting. Based on feedback at this TGDC meeting, NIST and the EAC identified several use cases for further exploration. NIST developed specific scenarios for these use cases, and has held several meetings with the Election Working Group chairs to further discuss and expand the use cases[7].

  - Pre-Election (79 members, 48 organizations)
  - Election (90 members, 58 organizations)
  - Post-Election (76 members, 45 organizations)

  Constituency Groups: The technical working groups were established in January 2016. The Interoperability Working Group carried over their activities from the IEEE Voting Systems Standards Committee effort and began meeting immediately. After

[4] Pre-election Process Functions and Model, http://collaborate.nist.gov/voting/bin/view/Voting/PreElection

[5] Election Process Functions and Model, http://collaborate.nist.gov/voting/bin/view/Voting/Election

[6] Post-election Process Functions and Model, http://collaborate.nist.gov/voting/bin/view/Voting/PostElection

[7] NIST Use Case Discussion Document, http://collaborate.nist.gov/voting/pub/Voting/VVSGStructure/nextgen-vvsg-scope.pdf

initial review of the use case and proposed structure[8] of the VVSG were discussed at the September 2016 TGDC meeting and the Constituency Working Groups are proceeding according to the feedback received regarding priorities.

- Interoperability Working Group (133 members, 78 organizations): Meets bi-weekly, with additional meeting for subgroups. NIST produced:
  - Election Results Reporting Specification[9]
  - (Draft) Election Event Logging Specification[10]
  - (Draft) Cast Vote Records Specification[11]
  - (Draft) Voter Registration Database Records Interchange[12]
  - Voting Glossary to Support Interoperability Standards[13]

  NIST continues to oversee additional efforts that were carried over from the IEEE.
  - Voting Variations Formal Definitions[14]
  - Election Business Process Modeling[15]

- Human Factors Working Group (82 members, 52 organizations): Since May 2016, this group began meeting bi-weekly with election officials, voting system designers, and usability and accessibility researchers and advocates to analyze the voting system technology requirements in VVSG 1.1 and recent drafts of the Roadmap and use case documents, and identify and develop new requirements for VVSG 2.0.
- Cybersecurity Working Group (85 members, 50 organizations): E-mail discussions and a summer 2016 kickoff meeting provided input for VVSG scoping discussions surrounding the NIST-developed use cases at the September 2016 TGDC meeting. The group is currently discussing one of the priority areas of the TGDC, remote ballot marking, and will begin bi-weekly meetings in Fall 2016.
- Testing and Certification Working Group (53 members, 32 organizations): The Testing and Certification Working Group had some early discussions surrounding test assertions and methods of automated test development. It will be the last group to get started, and will begin bi-weekly meetings in late Fall 2016 to discuss component based testing, quality assurance, configuration management, methods to test COTS, and testing of mandatory/optional features of the VVSG.

---

[8] VVSG Proposed Structure, http://collaborate.nist.gov/voting/pub/Voting/VVSGStructure/nextgen-vvsg-structure.pdf

[9] Election Results Reporting Specification: https://www.nist.gov/itl/voting/nist-election-results-common-data-format-specification

[10] Election Event Logging Specification: http://collaborate.nist.gov/voting/bin/view/Voting/ElectionEventLogging

[11] Cast Vote Records Specification: http://collaborate.nist.gov/voting/bin/view/Voting/BallotDefinition

[12] Voter Registration Database Records Interchange: http://collaborate.nist.gov/voting/bin/view/Voting/OnlineVoterRegistration

[13] Voting Glossary to Support Interoperability Standards: http://collaborate.nist.gov/voting/bin/view/Voting/Glossary

[14] *Voting Variations Formal Definitions: http://collaborate.nist.gov/voting/bin/view/Voting/VotingMethodsModels*

[15] *Election Business Process Modeling: http://collaborate.nist.gov/voting/bin/view/Voting/ElectionModeling*

5. Since the EAC needs to approve the voluntary voting system guidelines that the Technical Guidelines Development Committee (TGDC) develops, what did the TGDC produce in the years when there were no EAC Commissioners to approve anything?

NIST Response:
During the years where there were no EAC Commissioners, the TGDC did not meet due to the absence of the Designated Federal Officer. However, NIST continued to support the EAC and the Federal Voting Assistance Program, and reached out to NASED, local election officials, manufacturers, academics, and advocacy groups to better understand their requirements for the new VVSG 2.0.

a. Since the EAC was still funded during those years, and NIST continued to receive money from the EAC for elections work, how did NIST's use of the funds during this time benefit taxpayers?

NIST Response:
NIST continued to conduct research in security, human factors, interoperability, and testing, and applied this research in the development of guidelines for VVSG 1.1 and preparing for the development of guidelines for the new VVSG 2.0.

- **VVSG Development and Support:**
  - NIST developed two drafts for VVSG 1.1 and provided resolutions to comments resulting from two public comment periods. VVSG 1.1 was approved by the EAC Commissioners in March 2015, shortly after they were appointed.
  - NIST continued to provide support in interpreting VVSG 1.0 and developing further guidance for the EAC and VSTLs.
  - NIST's National Voluntary Laboratory Accreditation Program (NVLAP) conducted assessments for all three VSTLs.
- **Research:** NIST conducted foundational research in a number of areas in preparation for VVSG 2.0
  - **VVSG Goals, Scope & Structure**
    - Future of Voting Systems Symposia: NIST conducted two symposia in 2013 and 2015 aimed at sharing advances in election technology and identifying high priority areas for consideration in VVSG 2.0.
    - VVSG Structure: NIST worked closely with NASED, the Bipartisan Policy Center, and the Presidential Commission on Election Administration in identifying and prototyping a new structure for the VVSG, which advocated for high-level principles, guidelines, requirements and test assertions.
    - VVSG Goals: NIST participated in the EAC effort on defining goals for the VVSG 2.0.

- Military and Overseas Voters: NIST participated in the Council of State Government Technology Working Group to address ballot duplication, data standardization, and ballot delivery for military voters.

- **Security**
  - Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA): NIST conducted research for military and overseas voters, leading to three security publications:
    - *Security Considerations for Remote Electronic UOCAVA Voting* (NISTIR 7770)
    - *Information System Security Best Practices for UOCAVA-Supporting Systems* (NISTIR 7682)
    - *Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters* (NISTIR 7711)
  - Software Assurance:
    - NIST researched common software vulnerabilities and identified over 250 weaknesses in the areas of authentication, cryptography, input validation, and privilege management.
    - NIST developed test assertions for software requirements, VVSG 1.0.
    - NIST researched static and dynamic source code analyzers and developed customized automated tools to the VSTLs to aid in source code analysis of voting systems written in C, C++, and Java.

- **Human Factors**
  - Testing:
    - NIST conducted research into usability and accessibility performance test protocols, leading to new guidance for manufacturers and VSTL.
    - In response to an EAC request to augment testing for usability and accessibility, NIST developed and harmonized 589 test assertions with the VSTL's and the manufacturers.
  - Accessible Voting Technology:
    - NIST aided the EAC in identifying research topics and review grant submissions for the Accessible Voting Technology Initiative (AVTI) Grants Program, and held four webinars to share the research resulting from the grants with the community. NIST also developed an AVTI web portal as a repository of accessible voting research results.
  - Usable Security

- NIST directed research for the evaluation of usability of end-to-end encrypted voting systems.
- NIST conducted research and developed draft principles for secure and accessible remote ballot marking

  - Electronic Poll-book Usability: NIST conducted field analysis of electronic pollbooks and developed usability test protocol and associated checklist.
  - U&A Roadmap: NIST conducted two workshops and developed a roadmap that identified emerging technologies in elections, gaps in VVSG requirements, and suggested paths forward in defining requirements for VVSG 2.0.

- **Marginal Marks Research:** NIST conducted research in marginal marks, analyzed several collections of marked ballots, and wrote two white papers on the topic.
  - Development of Appropriate Test Markings for Optical Scan Voting Machines – **Phase 1**: Ballot Scanning and Collection
  - Development of Appropriate Test Markings for Optical Scan Voting Machines – **Phase 2**: Analysis of Ballot Markings

- **Common Data Format**
  - IEEE Committee:
    - NIST re-started IEEE working group P1622 for voting system common data format specifications and eventually broadened it to become a full IEEE committee.
    - NIST served as Chair of the IEEE P1622 and later IEEE VSSC Committee and actively recruited election officials, academics, manufacturers, and technical experts as members, significantly growing the effort.
    - NIST held four workshops to gather common data format (CDF) requirements from state election officials and develop support for CDF development goals from election officials, manufacturers, and election community at large.
    - NIST moved the IEEE work to the Interoperability Working Group to ensure that the standards remain freely available to election officials and manufacturers and provide for a more agile effort.

  - Standards:
    - NIST supported development of 1622-2011, IEEE Standard for Electronic Distribution of Blank Ballots for Voting Systems
    - NIST issued Special Publication 1500-100 *Election Results Reporting CDF Specification*
    - NIST completed draft Special Publication 1500-101 *Election Event Logging CDF Specification*

- NIST developed initial CDF specification for Online Voter Registration for use with National Voter Registration Act and Federal Post Card Application registration on-line forms
- NIST developed initial CDF specification for Cast Vote Records export from ballot scanners.

- Outreach:
  - NIST assisted the State of Ohio in their implementation of Special Publication 1500-100 for election results reporting, used in 2015-2016 elections
  - Working with Google, NIST unified the Special Publication 1500-100 format with Pew's Voting Information Project Version 5.0 format.

6. Why, in an age of rapidly advancing technology, has the EAC and NIST, working together for over a decade, achieved only one upgrade in voting system guidelines, and only one large enough to be called VVSG 1.1, versus 2.0, after 10 years? Should we expect that the next iteration of voluntary voter system guidance (VVSG) will not take as long to be released? When do you expect that to be?

NIST Response:
Following the adoption of the VVSG 1.0 in 2005, NIST worked with the TGDC on revised guidelines that included across-the-board improvements, addressing human factors, reliability, auditing, software quality, and security. This version, now referred to as the 2007 TGDC draft, was not adopted by the EAC due to significant concerns regarding the cost in updating and testing voting systems, as well as key recommendations on vulnerability testing and software independence. The EAC expressed a desire to instead update the 2005 VVSG 1.0 recommendations to incorporate lessons learned via the testing and certification process and aspects of the 2007 TGDC draft that did not require hardware changes, significant changes in format in the VVSG, or significant changes to software. NIST worked with the EAC to develop a draft VVSG 1.1, which went out for public comment in 2011 but was not adopted due to a lack of a quorum of EAC Commissioners. Between 2011 and 2015, the EAC and NIST updated this version to incorporate additional security and testing guidelines, and went through a final comment/resolution process. When the EAC Commissioners were confirmed in 2015, the VVSG 1.1 was approved.

NIST has introduced the use of the Voting Public Working Groups to develop the draft requirements for the VVSG 2.0, to ensure broad-based community support for the new standards. NIST anticipates a draft version of the guidelines in FY2018.

a. Should the process be changed so that it doesn't take as long to update the guidelines?

NIST Response:
HAVA places the responsibility for the development of draft VVSG on the TGDC and NIST, serving in its capacity as the technical arm of the TGDC. After acceptance of the draft guidelines, the EAC is required to get feedback from its Standards Board, the EAC

Board of Advisors, and the public through robust comment periods. Depending on that feedback, assumptions made at the onset of the guideline development process may change, thus requiring significant rewrites.

Typical standards efforts proceed by providing all stakeholders an opportunity to participate in the development process, thereby achieving consensus and buy-in early on, with continuous engagement throughout the development of the standard.

NIST has addressed early engagement of stakeholders through the establishment of the Voting Public Working Groups. Currently, working group membership suggests that stakeholders are engaging in the development process. However, this environment differs significantly from other standards efforts, in that most of the members are volunteers. To date, NIST has provided much of the technical development, with members commenting on NIST-developed materials. Success will depend upon true engagement and participation by stakeholders in this process.

b. Are there any states that fully implement the guidelines?

NIST Response:
The VVSG are voluntary for use by the states and often dictated by state laws. There are several categories of use of either the guidelines themselves, the VSTL that are accredited by NVLAP and approved for use by the EAC, or the EAC certification process. In a July 2015 TGDC meeting[16], Tammy Patrick, Bipartisan Policy Center, indicated that 47/50 states use some portion of these as follows:

- Relevant state statutes and/or rules require that voting systems be certified by a federal agency in 13 states. Those states are CO, DE, GA, ID, NC, ND, OH, SC, SD, UT, WA, WV, and WY.
- Thirteen states require voting systems be tested by a federally approved/accredited laboratory. Those states are AL, AZ, IL, IA, LA, MA, MD, MN, MO, NM, PA, RI, and WI.
- Nine states and the District of Columbia require testing to Federal standards. Those states are CT, HI, IN, KY, NV, NY, TN, TX, and VA.
- Further, some states use parts of the Federal Standards or Certification as follows:
    - Standards
        - AK, AR, KS, MI and MS semantically refer to Federal Standards (i.e., HAVA, FEC, NASED).
        - For California, Federal Standards set a minimum threshold for their standards.
        - Florida uses large portions of the VVSG.
        - New Hampshire does not have a statutory set of standards but will use sections of the VVSG as well as looking at what other states equipment is certified in and how they tested it.
    - Certification

[16] TGDC Informational Meeting, July 2015, https://www.nist.gov/itl/presenations-tgdc-meeting-july-20-21-2015

- While not required in statue, Nebraska does require Federal certification before a system can be used in their state. They require Federal certification through internal policy.
- Maine does not require Federal testing by statute but required EAC certification in their last request for proposals.
- Statutorily, Montana does not have to have Federal certification prior to certifying a voting system for use in Montana. However, as a practical matter they have always relied on the testing that goes into Federal certification.
- New Jersey does require testing to the Federal guidelines. It is not in statute but rather a de facto requirement established by the voting machine examination committee.

7. Have states fared well without timely updates to the voluntary voter system guidance (VVSG)? If so, is there an argument to be made that NIST no longer needs to play a part in providing technical guidance for voting systems?

NIST Response:
States have come to rely upon on the Federal guidelines, accredited testing laboratories, and the associated testing and certification processes. Thirty-five states require Federal certification or testing, with 47 states in total using some portion of the Federal program to assess the voting systems used within their states. Reports from the PCEA, NIST engagement with NASED, the TGDC, and the working groups suggest that states are looking for additional guidance beyond the original scope of casting and counting ballots, particularly in applying emerging research in usability and accessibility to new technologies, such as tablets and iPads, in network and web-based security, and in the development of common data formats.

8. Do you believe that the voluntary voter system guidance (VVSG) should be updated to incorporate the security of online voter registration systems, electronic poll books, electronic ballot marking, ballot on demand, ballot delivery, election reporting, and auditing?

NIST Response:
From a technical perspective, all of these technologies would benefit by being included in the scope of the VVSG and thus subject to security and penetration testing by VSTLs. At the same time, a larger scope will increase the time needed to develop new guidelines and greater testing may drive up the costs of the systems. Further, those systems that connect to networks still need to be monitored and tested periodically as they are used and updated to mitigate new vulnerabilities. Thus, including them in the scope of the VVSG may help but is not, by itself, sufficient for improving their security.

   a. Why has it taken this long to address these other aspects of election systems?

   NIST Response:

The VVSG have been historically limited in scope to the activation of the ballot, casting of ballots in polling places, and counting ballots. Recent advances in technology have provided new methods for checking in voters, identifying appropriate ballots for voters, and marking the ballots through the use of iPads and tablets. At the same time, voting has expanded beyond the polling place to vote centers and in some cases, to the home where ballots can be marked remotely using online ballot marking tools. Many of these technologies are becoming more widely available to states, in an effort to replace what was traditionally paper-based processes with electronic alternatives.

Following the February 2016 TGDC meeting and a review of the process models developed by NIST, the EAC indicated that the scope for VVSG 2.0 would not be expanded and would remain limited to ballot activation, casting, and counting. Due to the increased awareness of security issues affecting both voting and election systems, and the in-depth review of NIST developed use cases, the TGDC voted unanimously at the September 2016 meeting to consider developing requirements for these technologies, with the exception of voter registration.

Although NIST is proceeding with the development of guidelines based on TGDC priorities, the final decision on what is included in VVSG 2.0 is yet to be determined and will be discussed at future TGDC meetings. Ultimately, the draft VVSG 2.0 recommendations will be forwarded to the EAC for final approval. States are responsible for determining whether the new requirements will meet the needs of their voters.

9. Has NIST studied the vulnerabilities of states' voter registration databases, of Internet voting, of electronic pollbooks, and other aspects of election systems? Has NIST provided technical advice and guidance for states to help protect these aspects of their election systems? If not, why not?

NIST Response:
NIST scientists have been conducting research into the use of electronic technologies to support overseas and military voting, including casting ballots over the Internet. NISTIR 7551, A Threat Analysis on UOCAVA Voting Systems, analyzed the use of several electronic technologies for different aspects of the absentee voting process. This research concluded that widely-deployed security technologies and procedures could mitigate many of the risks associated with electronic ballot delivery, but that the risks associated with casting ballots over the Internet were more serious and challenging to overcome.

Based on that research, NIST developed two documents covering security best practices for UOCAVA voting, NISTIR 7711, Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters and NISTIR 7682, Information System Security Best Practices for UOCAVA-Supporting Systems. These two documents serve as companion documents to one another. NISTIR 7711 covers security best practices and considerations for election officials considering the use of electronic mail or Web sites to expedite transmission of voter registration materials and blank ballots. NISTIR 7682 provides best practices for IT professionals charged with configuring and administering IT systems used to support UOCAVA voting.

NIST also developed NISTIR 7770, Security Considerations for Remote Electronic UOCAVA Voting, which studied Internet voting in more detail. This report identified and analyzed current and emerging technologies that may mitigate risks to Internet voting. It also identified several areas that require additional research and technological improvements.

10. Do states reach out to NIST for election technology assistance and guidance? How often does this occur and in what capacity?

NIST Response:
NIST, as directed by HAVA, serves as the technical arm for the TGDC, and in particular, conducts research and develops draft guidelines for voting systems. In this capacity, NIST has interacted with the states through NIST-sponsored workshops, and provided guidance through published materials and presentations to organizations such as NASED. For the common data format work, NIST has been interacting with a number of the states in discussions about their voting device infrastructures and how their elections are conducted, so as to develop common data formats that work across all states. Some of the states that NIST has interacted with most frequently include Ohio, Wisconsin, New York, California, North Carolina, West Virginia, and Maryland. Specific assistance for an individual state is only occasionally asked for and provided by NIST. The EAC serves as a clearinghouse for election-related information.

11. What is NIST doing, in collaboration with DHS, if anything, to assist the States for beyond 2016?

NIST Response:
NIST is working with the Department of Homeland Security (DHS), Department of Justice, and EAC to ensure that federal government efforts are properly coordinated and identify the services, guidelines and tools NIST could provide election officials to help improve the security of their systems. This includes making sure election officials are aware of existing resources that are available to help them today. These include the guidelines and best practices that exist for voting and other IT systems from NIST, EAC and DHS, cyber hygiene scanning services by DHS, and threat and vulnerability bulletins from DHS and FBI. This is an on-going effort that will take into account the feedback NIST receives from election officials on what types of assistance will best address their needs.

12. What specific technical measures is NIST providing to help States better understand and measure their gaps and understand their cyber hygiene?

NIST Response:
While NIST's work on the VVSG has been focused on voting equipment used to capture and count votes, NIST has a broad set of cybersecurity standards and guidelines that state and local election officials can use to protect voter registration systems and other IT systems that support elections. These standards and guidelines cover risk management, contingency planning and incident response, web server security, and cryptography.

In addition, the Cybersecurity Framework containing voluntary guidance based on existing standards, guidelines, and practices can help state and local election officials better understand and manage risks in their election systems.

a. Does NIST work in collaboration with DHS on this?

NIST Response:
NIST has a longstanding collaboration with DHS on cybersecurity, including the Cybersecurity Framework, and more recently has worked with DHS to identify what services, guidelines and tools NIST could provide election officials to secure their systems. NIST will continue to work cooperatively with DHS as well as the Department of Justice to ensure that federal government efforts are properly coordinated.

b. Do States conduct some sort of stress test on their systems? If not, should they?

NIST Response:
The VVSG 1.1 includes volume and stress testing to evaluate the voting device's response to processing more than the expected volume of ballots/voters and determine whether the hardware and software operate accurately and continuously under high rates of ballot processing. During these tests, the accuracy of the voting system as it records voter choices and tabulates ballots is measured and evaluated. The tests also include stressing the hardware, such as evaluating the device's response to wide ranges of temperature and humidity as well as the device's capability to withstand common issues such as voltage spikes and loss of power/operation on battery power. Some states such as California have conducted their own volume and stress testing, but states generally rely on the testing required for EAC certification, i.e., from the VVSG.

13. Is NIST conducting any research on internet voting?

NIST Response:
NIST has extensively studied Internet voting as part of NIST's work under the Military and Overseas Voter Empowerment Act to support the EAC and Federal Voting Assistance Program in their missions to help overseas and military voters exercise their right to vote. This research, documented in NISTIR 7551 and NISTIR 7770, identified and analyzed the significant security challenges in voting over the Internet securely, and discussed security technologies and research that may be able to address these challenges. As part of the priority suggestions from the September TGDC meeting, NIST will conduct additional research on the use of the Internet in the voting process, including for blank ballot delivery and online ballot marking.

a. What prospects does NIST foresee for secure voting over the Internet?

NIST Response:
NIST'S research in the security of Internet voting found significant security challenges with Internet voting at scale. The need to protect the integrity of cast votes, while also

protecting voter privacy, makes Internet voting fundamentally different from other transactions online.

However, it is important to look at these risks in context. The vast majority of states that allow some form of Internet voting do so for some portion of the overseas and military voters covered by the Uniformed and Overseas Citizen Absentee Voting Act (UOCAVA). These voters face real challenges obtaining and returning their ballots in time to be counted. States must balance the risks of Internet voting against the possibility of disenfranchising overseas and military voters.

14. Some experts have stated that the paper ballot is in and of itself secure. Do you agree with that statement?

NIST Response:
Electronic voting machines provide significant advantages over hand-marked paper ballots. For example, electronic systems provide accessibility features required by HAVA and help prevent errors in marking the ballot.

Many voting systems in use today produce a paper record in the voting process. A voter verifiable paper record can provide an independent record that can be compared against electronic records or tallies produced by the voting system. These records can help verify that voting systems operated correctly in an election, and to identify the cause if they have not a property of voting systems known as auditability. However, paper is not an accessible technology, and may prevent a voter with certain disabilities, such as vision loss, to vote privately and independently. However, there is tension between the voter-verifiable and auditing capabilities that paper provides and the difficulty paper poses to voters with certain disabilities to vote privately and independently.

Many jurisdictions are now using optical scan paper ballots. These ballots are paper and are marked, either by hand or by using an electronic ballot marking device which prints out the ballot. The ballots are counted using an optical scan machine. Direct-Record Electronic machines, also known as touch-screen voting machines, are still used in a few states and some of these systems also produce a paper record.

It is ultimately up to state and local election officials to determine what voting systems will best accommodate voters in their jurisdictions.

a. Do you believe that paper ballots are the most secure mode of casting a vote during a time of multiplying cyber threats?

NIST Response:
There are security risks with any voting method and election system. When assessing the security of a system, it is important to consider the complete voting process, taking into account the technical and procedural controls in place to protect the integrity of the election.

15. Given that the newly established Presidential Commission on Enhancing National Cybersecurity established this past year by Executive Order is charged with delivering to the President a report with a goal of "strengthening cybersecurity in both the public and private sectors while protecting privacy, ensuring public safety and economic and national security, fostering discovery and development of new technical solutions, and bolstering partnerships between Federal, State, and local government and the private sector in the development, promotion, and use of cybersecurity technologies, policies, and best practices," what specific measures is NIST undertaking to ensure lessons learned from these efforts are shared with the Department of Commerce -which is serving as the Executive Agent?

NIST Response:
NIST, a bureau in the Department of Commerce, provides leadership and technical expertise to other Commerce-led efforts including the Internet Policy Task Force, the Commerce Department's Digital Economy Agenda and Skills for Business initiative, and other multi-stakeholder processes. Our contributions are informed by our technical expertise; our long-standing role to develop cybersecurity standards, guidelines, and practices; our collaborations with diverse stakeholders from government, industry, and academia; and lessons learned from cybersecurity programs including the Cybersecurity Framework and the Commission on Enhancing National Cybersecurity. The lessons learned as a result of NIST's support to the Commission will also inform NIST's current and future cybersecurity research agenda.

a. Will the Commission address the cybersecurity of voting and election systems technology?

NIST Response:
The Commission on Enhancing National Cybersecurity is a Federal advisory committee that will independently provide short-term and long-term recommendations to the President to strengthen cybersecurity in Federal, State, and local government and private industry, and across all sectors of the digital economy.

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

"Protecting the 2016 Elections from Cyber and Voting Machine Attacks"

Dr. Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology (NIST)

Questions submitted by Rep. Eddie Bernice Johnson, Ranking Member

1. The 2014 Presidential Commission on Election Administration recommended that the standard-setting and certification process for new voting technology should be reformed in order to encourage innovation and to facilitate the adoption of widely available, off- the-shelf technologies and 'software-only' solutions. How is NIST responding to this recommendation and/or assisting the EAC in responding to this recommendation? How can you balance the need for minimum security and accessibility standards with promoting innovation?

NIST Response:
Using commercial off-the-shelf (COTS) products and software-only solutions as components of a voting system poses challenges to the EAC testing program in that the source code for the technologies may not be available for inspection and the lifecycle of the technologies may be difficult to predict, e.g., some products may be off the marketplace in a relatively short number of years. The EAC is using a part of the VVSG known as the extensions clause in order to extend the scope of the VVSG requirements to COTS products and software-only solutions and working with the test labs to arrive at approaches for providing adequate testing to these technologies. An important factor in the EAC decision whether to allow these technologies as components of the voting system deals with how the technology is being employed, that is, whether changes to the technology would have a large or relatively small impact to the voting system.

One of the primary purposes of the NIST common data format (CDF) work is to promote interoperability of components within the voting system and those that interface to the voting system. The use of a CDF permits greater use of COTS and software-only technologies in that the distinction between vendor-proprietary components and COTS/software-only technologies is largely erased when an interoperable format is used for data import and export. For example, if a COTS tablet device is used as a ballot marking device, the electronic records on the tablet can be exported from the device in an interoperable format and subsequently used in audits and tabulations, whereas if proprietary data formats are used, COTS is made more difficult to interface.

Balancing requirements for security and accessibility without unduly restraining innovation is fundamentally important and NIST has addressed this by developing requirements and test methods that focus on performance of the voting system components as opposed to the specific design of the components. At the same time, laws dealing with accessibility cannot be ignored and security/integrity issues affecting network-based components are increasingly serious. When evaluating COTS products for use as part of the voting system, how well the

products deal with these issues is examined and used to arrive at a decision whether to permit use of the products.

2. There are currently three accredited Voting System Test Laboratories. Can you discuss NIST's efforts to monitor and review the performance of the laboratories accredited by the Elections Assistance Commission? What is the process for making recommendations for continuing accreditation? Does NIST continue to track the reliability of voting technology certified by these Labs? What are the challenges to accredit additional private labs?

NIST Response:
NIST inspects the VSTLs using NVLAP, which inspects and accredits labs in a variety of areas besides voting, such as medical and electronics. The inspections may occur at one-two year intervals, and cover areas such as the basic adherence of the lab to industry-standard ISO specifications as well as items specific to voting, including conformance to requirements in the VVSG and EAC certification program manuals. Labs must report back to NVLAP if there are changes to their testing programs and NVLAP may require increased inspections depending on feedback from the EAC.

NIST recommends the NVLAP-accredited labs to the EAC, and the EAC subsequently votes on whether to certify the labs as VSTLs. The EAC may require additional criteria of the labs. NIST does not monitor the performance of voting devices that have been EAC-certified; the EAC does provide a method for voting offices to report on issues with the reliability of their EAC-certified voting technology, and this information is fed back into the NIST NVLAP inspection process. The challenges to accrediting additional private labs to the NVLAP criteria include the labs acquiring the necessary expertise in voting technology, testing voting systems, and specialized knowledge in areas such as usability, accessibility, and security, especially penetration testing and system hardening against attack.

3. One issue you discussed in your testimony is the need for greater interoperability across voting systems developed by different vendors so states and jurisdictions have more choices in the marketplace. Please expand on the benefits and challenges of creating a common data format for election data and NIST's work in developing the standard.

NIST Response:
A common data format (CDF) has the benefits of achieving common understandings and definitions of the data across all states, and then a common format for importing and exporting the data to/from voting devices. In the case of election reporting or voter registration data, the common format enables a variety of manufacturers and election officials to import and export data in an interoperable way into and out of the collection of devices NIST calls the voting system. Within the voting system, common data formats used between and among the devices can achieve some interoperability and thus allow the voting system to be composed of devices produced by a variety of manufacturers as opposed to only the same manufacturer. This opens the market to more manufacturers and will ultimately result in greater choice by election officials and, likely, more competition and higher quality.

NIST led the creation of an IEEE committee to focus on CDF development along with state officials and others from the voting community, and has since moved the work to the Interoperability Working Group so as to increase participation and make the formats available freely. NIST typically develops use cases for the formats with the assistance of the working group members, and then develops the formats and works with states and others to field test the formats and create final versions. NIST has worked closely with Ohio and more recently North Carolina to integrate the election results CDF into their respective IT structures, and has worked with states and manufacturers in its development of formats for logging, voter registration, and electronic cast vote records, among other efforts.

4. In your testimony, you discussed the human factors technical working group. Can you elaborate on the role of human factors in elections systems technology research and standards development?

NIST Response:
Human factors plays a key role in election systems technology, ensuring that every voter is able to mark and cast a ballot as they intend, independently and privately, during an election. This principle was set forth in HAVA, and is foundational to NIST's work on usability and accessibility. NIST's scope includes not just access for people with disabilities but ease of use for all voters who have a range of capabilities (e.g., voters with low literacy, aging voters, voters for whom English is not their native language, etc.).

Responses by Hon. Tom Schedler

HOUSE COMMITTEE ON SCIENCE, SPACE AND TECHNOLOGY

"Protecting the 2016 Elections from Cyber and Voting Machine Attacks"

Hon. Tom Schedler, Secretary of State, State of Louisiana Secretary of State

Questions submitted by Rep. Lamar Smith, Chairman

1. Are the touch-screen electronic voting machines that are in use in most states the best and most secure available systems on the market today?
   Speaking only on behalf of the State of Louisiana, our touch-screen voting machines are secure and have the most up-to-date software available on the market. Louisiana is currently engaged in the process of securing an appropriation (whether federal or state) to update our voting machines, however cost is always a factor in states being able to purchase the most secure available systems on the market today.
   a. Are manufacturers still supporting patches and upgrades to states? In Louisiana's case, Yes.
   b. Do you know if voting machine manufacturers plan major upgrades in the near future? I would refer this question to the manufacturers or the Elections Assistance Commission.
   c. Has the EAC or have the states sat down with voting machines manufacturers to discuss how to upgrade technology and address vulnerabilities? Louisiana has had discussions with its voting machine manufacturers. I would refer the EAC question to them.

2. Do you think the 2016 elections would be more reliable if most states and local jurisdictions were still relying on paper ballots? Absolutely no. Paper ballots are not inherently superior to voting machines. No part of the vote counting process is done online and all our voting machines are standalone units that are never connected to the Internet. In fact, the vast amount of historical evidence shows the most common source of voter fraud is paper ballots submitted through the absentee voting process.

3. In retrospect, has HAVA been a net plus or a net minus? Since most states, including Louisiana, used HAVA dollars in 2005-2006 to upgrade their voting systems, I would conclude it has been a net plus and I would encourage Congress to look at ways to provide another similar appropriation to states in the near future to support our efforts to again upgrade our voting systems.

4. How effective do states, or at least the state of Louisiana, find NIST's work in proving technical guidance? Do states use this guidance or use NIST as a resource in securing

their systems? If not, why not? Louisiana uses NIST standards for technical guidance and find them to be a valuable resource.

a. What technological areas should NIST prioritize in order to strengthen election cyber security? One way to strengthen elections in the future could be a partnership between NIST and EAC to provide ongoing assistance to states by identifying the kind of testing that would reveal signs of tampering that a sophisticated nation-state adversary might conduct on election systems.

5. Given the heightened attention to election security this year, are states doing anything different as they prepare for this Presidential Election? Louisiana's election system was secure before this election cycle and remains secure for the Presidential Election cycle. There are multiple layers of protection in place as well as checks and balances available to our election administrators that ensure the integrity of the election outcome.

   Without question, states are on high alert for cyber threats in this voting cycle, but it is important to remember that there is always contingency planning around manmade and natural threats to election. For instance, in Louisiana, some 65 precincts impacting approximately 65,000 voters were destroyed/damaged due to historical flooding in August. Other states, impacted by Hurricane Matthew have had to implement emergency voting plans for impacted citizens just as Louisiana did in the aftermath of Hurricane Katrina.

   States are deploying numerous resources for this election cycle including extensive testing for cyber threats outlined in recent federal alerts. States will continue testing their systems in the run-up to Election Day in order to keep them defended. Additional steps could be taken based up any credible or specific threats that are identified. Secretaries of State are also taking part in a Department of Homeland Security Election Infrastructure Cybersecurity Working Group, created for sharing resources and best practices.

6. What is your biggest concern as you prepare for the November election in Louisiana? The information being communicated to the public concerning the security of election systems and voting machines have reached the level of unnecessary public alarm. To be blunt, some are misleading voters to believe their vote won't count and that is extremely irresponsible given the facts. Voter fraud is much, much harder to accomplish than you think and would require a lot of people breaking federal and state laws simultaneously without detection to impact the outcome of a national election. The best we can do is create as many barriers and safeguards as we can against stealing an election. And we have. It's important to note, the complexity of our election system in this case has reinforced the integrity of the process.

7. Following news reports about the Arizona and Illinois breaches of voter registration databases, the FBI has warned states to conduct vulnerability scans. Has Louisiana heeded this warning? Do you know if other states have?
Louisiana, as well as many other states, have conducted vulnerability scans.

8. Elections typically bring about stories and allegations about one political party trying to manipulate the system in the candidate's favor. Is it conceivable that such action could extend to one party electronically attacking or attempting to hack into voting and election systems to benefit their candidate of choice?
Speaking only for Louisiana, we take all scenarios seriously and will continue to take a proactive approach to maintain the integrity of our election process. Additionally, we work closely year round with both major political parties to forge relationships that benefit ALL voters in our state. We share monthly reports on voter registration/demographics and meet before every major election to discuss the best ways to share election night information and results. The role of the Secretary of State is to forge strong partnerships with all entities involved in the election process through communication and transparency.

Responses by Mr. David Becker

SUPPLEMENTAL TESTIMONY FROM DAVID J. BECKER,

EXECUTIVE DIRECTOR, THE CENTER FOR ELECTION INNOVATION & RESEARCH

OCTOBER 28, 2016

RESPONSES TO QUESTIONS FROM CHAIRMAN LAMAR SMITH,

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

1. Elections typically bring about stories and allegations about one political party trying to manipulate the system in their candidate's favor. Is it conceivable that such action could extend to one party electronically attacking or attempting to hack into voting and election systems to benefit their candidate of choice?

   While it is not inconceivable that one party could consider or attempt to electronically hack into systems to achieve an advantage, in general, I believe there are adequate protections in place to deter and prevent such an attempt. Throughout the nation, processes surrounding elections are made transparent, and are particularly open to review from the parties, thus making it extremely unlikely that partisans could achieve a hack without being compromised or noticed by another party.

2. In retrospect, has HAVA been a net plus or net minus?

   In retrospect, HAVA has been a big net plus. The funding to the states for new voting systems has helped greatly, though an even more regular source of funds for upgrading and purchasing new voting systems would help even more. In addition, the requirement that each state maintain a statewide voter registration database has led to a major improvement in the accuracy of voter lists and improved efficiencies, while also paving the way for significant and positive reforms like online voter registration and membership in the Electronic Registration Information Center (ERIC), both of which have contributed to more accurate and inclusive voter lists.

3. What technological areas should NIST prioritize in order to strengthen election cybersecurity?
   I have no specific recommendations on this issue.

4. Some experts have stated that the paper ballot is in and of itself secure. Do you agree with that statement?
   a. Do you believe that paper ballots are the most secure mode of casting a vote during a time of multiplying cyber threats?

   I believe that paper ballots, with technology as it exists at the current time, can add to security when combined with post-election audits. Of course, there are other considerations in voting, such as accessibility and usability as well.

RESPONSES TO QUESTIONS FROM REP. EDDIE BERNICE JOHNSON,

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

1. In response to a recommendation by the Presidential Commission on Election Administration, the CalTech/MIT Voting Technology Project developed a web site that elections officials can use to determine if they can deploy a more efficient line management configuration to help shorten lines. The project highlighted the science of line management and queuing theory. What other areas of election and voting science and technology should Congress, particularly this Committee, look to support?

   It could be quite helpful if Congress looked to further support the following work:
   - Continuing the work of the Election Assistance Commission in providing technological advice and support, and certification of voting equipment. This work is very important.
   - Considering a long-term funding mechanism to assist jurisdictions in maintaining and obtaining the best technology to support our democracy infrastructure.

RESPONSES TO QUESTIONS FROM REP. ELIZABETH ESTY,

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

1. In your testimony, you describe four characteristics that make a voting system impervious to cyberattacks: a system that is highly decentralized, one where voting machines are kept secure and have no connection to the internet, with a paper record and audit requirements, not unlike the one we see in Connecticut. Given the recent hacks, not to mention in the backdrop of a presidential election year, the Department of Homeland Security is considering classifying the U.S. election system as part of the nation's critical infrastructure.
    a. How would this classification protect our election infrastructure?
    b. It's my understanding this classification would bring voting systems under Department of Homeland Security's cyber protection umbrella. Can you compare this approach to the ideal voting system you described earlier?
    c. As founder of the Electronic Registration Information Center (ERIC), can you explain how states like Connecticut have benefited from having a more accurate voter registry list?

Without more information about how a classification of our election system as critical infrastructure would impact how our elections are currently run and supported, it is difficult to express an opinion on how this would protect our elections. I will note that the federal government (including Homeland Security, the FBI, and others), state election offices, and local election offices, have cooperated admirably this election cycle, in response to both real and perceived threats, and I would expect such voluntary cooperation to continue, regardless of the classification.

As to ERIC, the 20 states and the District of Columbia, that participate in it, including Connecticut, have benefited a great deal. To date, collectively these states have accomplished the following as a result of their ERIC membership:

- Identified nearly 5 million voter records that were out of date due to a voter moving out of state or within the same state;
- Identified over 160,000 voters who had died since they last voted;
- Registered nearly 1 million new eligible voters who were not yet registered, usually via efficient and cost-effective online voter registration.

And these numbers will continue to grow, as more states join and use the ERIC data. For this reason, the Presidential Commission on Election Administration recommended that states join ERIC, and the Government Accountability Office reported that "a state's participation in ERIC leads to more accurate voter registration lists and cost savings for state and local election offices." The report can be found at http://www.gao.gov/products/GAO-16-630.

Responses by Dr. Dan S. Wallach

Written Q&A for Dr. Dan S. Wallach

Professor, Department of Computer Science

Rice Scholar, Baker Institute for Public Policy

Rice University, Houston, Texas

Following the House Committee on Space, Science & Technology Hearing,

"Protecting the 2016 Elections from Cyber and Voting Machine Attacks"

Hearing date: September 13, 2016

Questions submitted by Rep. Lamar Smith

1. How would you rank the vulnerability of the following: paper ballots, electronic voting machines with a paper ballot trail, electronic voting machines without a paper ballot trail, optical scan systems, and Internet voting?

From worst to best: Internet voting, electronic voting without a paper trail, electronic voting with a paper trail, paper ballots (centrally tallied), paper ballots with a precinct-based optical scanner.

Internet voting, in all of its current commercial forms, is not suitable for use in Federal elections. Given our understanding of the capabilities of the nation-state adversaries that an Internet voting system might face, we cannot guarantee the integrity and privacy of the vote, nor can we ensure the availability of the infrastructure supporting an Internet election.

The rest of my ranking generally favors paper ballots, with an extra edge to paper ballots which are scanned and tabulated in the local precinct. This configuration creates electronic records, suitable for rapid election night results. Furthermore, by having redundant electronic and paper records, we can conduct post-election audits that can detect (and thus deter) ballot-box stuffing or electronic data tampering.

2. Is the diffusion of our voting infrastructure across 50 states and nearly 10,000 localities a substantial impediment to cyber-attacks and hacking?

While this is an important benefit to the security of our election systems, there are a small number of vendors whose voting systems and/or voter registration database systems are widely used. An attack that was engineered to compromise one such system would be likely to work against other copies of the same system. Furthermore, an adversary who wished to tamper with our nation's elections need not tamper with each and every locality in order to flip the outcome. We would expect such adversaries to focus their efforts on battleground states, particularly the largest counties in those states where more votes are cast.

3. It has been said that a graduate student in computer science could figure out how to hack into an electronic voting machine. Do you believe that this is something that could happen this upcoming election, with the student's actions leading to a change in an election result?

Prior studies of election security sponsored by the states of California, Ohio, and Florida were conducted by a mix of industrial professionals, professors, and graduate students. Based on the findings of these studies, and my participation in the California Top to Bottom Review, I

estimate that an engineering team of this sort with access to working voting machines, but not given access to the source code to those machines, would require roughly 6 man-months of effort to discover relevant vulnerabilities and craft suitable cyber-attack tools. Once such tools were crafted, the next challenge would be inserting them into a live election. The details for how to do this would obviously vary from one system to another, but would be greatly aided by the common practice of election officials staging their equipment in the field in advance. (This is colloquially referred to as the "sleepover problem", and is a direct consequence of the logistical challenges of managing the distribution of election equipment.)

4. What do you suggest is the most important thing that the states can do between now and the November elections to ensure that voting runs as smoothly as possible?

I have two specific recommendations. First, states and counties should request the assistance of federal cyber-investigators from DHS, FBI, and other such agencies, or from private companies that similarly specialize in auditing computer networks for intrusions. If lucky, they may discover latent attacks prior to the election, allowing for the possibility of specific pre-election mitigations. But, in the event that nothing is found, my second recommendation is for states and counties to produce detailed contingency plans for how they may recover from a "cyber disaster", should it occur. Having such plans, detailed in advance and agreed to by all parties, might dissuade attackers, knowing that the impact of their cyber attacks would be mitigated.

5. How can we better enable our overseas and military voters to securely cast their ballots?

My preference is that overseas and military voters be provided with "kiosk" polling places in embassies, consulates, and military bases. The design of a voting kiosk might be very similar to the design of a traditional polling-place voting system, except the return of voted ballots would be more complicated. Such a system might return ballots simultaneously through a combination of electronic means (using sophisticated cryptography) and traditional means (overnight couriers, etc.). Doing this properly requires having standards for how data is exchanged---a requirement where NIST has a natural role to play. We're still many years away from this being a reality.

At present, it should be noted that with the passage of the Military and Overseas Voter Empowerment (MOVE) Act in 2009, the "time and distance" problem for military voters has been greatly mitigated without requiring that voters risk secrecy and security by sending voted ballots over the Internet. Local election officials send requested ballots 45 days in advance of Election Day, voters can receive blank ballots electronically that same day, and military voters can use a special return label for trackable express ballot return that typically gets voted ballots back to the county official in 5-6 days. Half the states allow late-arriving military ballots to be counted if sent in a timely fashion.

6. Is there a way that we can use sophisticated cryptography, such as blockchain, to submit secure votes?

Cryptographic block chain technologies are an important ingredient in the design of secure electronic voting technologies. However, they do not represent a "silver bullet" with respect to solving all of the problems that arise with Internet voting. We simply do not have all the necessary technologies to guarantee voter privacy, ballot integrity, and election availability in the face of a determined adversary. I estimate that we are at least ten years away from the possibility of such a system, with significant unsolved and open research challenges standing between us and any such system being suitable for real-world use.

7. Is there enough research and development being undertaken in the security of voting and election systems?
    a. What technological areas should NIST prioritize in order to strengthen election cybersecurity?

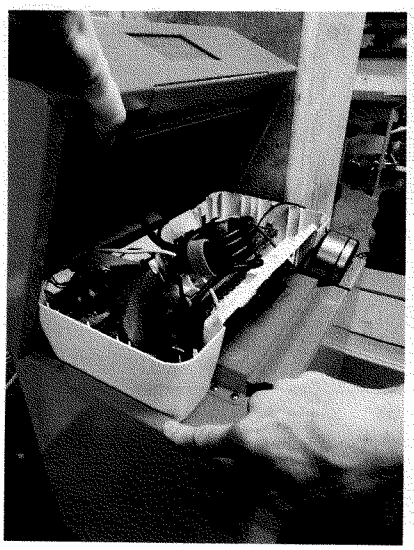
The National Science Foundation supports my own research in this area, as well as that of many of my colleagues, but there are no large efforts akin to DARPA's "grand challenges" being pursued at this time by any Federal agencies. The two most promising efforts, at the present time, are being pursued by Los Angeles County, California and Travis County (Austin), Texas. I'm personally engaged with the Travis County effort, and my understanding is that Federal funding could significantly accelerate their development process, which would yield an "open source" implementation that could then be shared with other counties and states.

NIST and the EAC can play an important role in ensuring that the technologies developed in LA and Travis counties be suitable for other counties and states, both by directly funding these efforts (and, thus, accelerating their development) and by identifying other counties and states who might be amenable to adopting these new systems, collecting and organizing their requirements such that the development efforts will address them. Furthermore, they can ensure that the voting system standards, currently being updated, avoid presenting unnecessary barriers to these new machines, while raising the bar to rule out the older generation of insecure devices.

8. Given the criticisms you and others have made about the security of voting machines, going so far as to call the coding in one particular manufacturer's machine "unacceptable", should more stringent testing have been conducted of these machines by either NIST or the EAC prior to approval for use by states?

The current "voluntary voting system guidelines" have the conundrum of making very detailed requirements of vendors' systems, while making negligible requirements of vendors' engineering processes. Problems that are only discovered late in the engineering process are more expensive to fix, particularly if those problems are a result of poor engineering decisions made early in a system's design process. This is a recognized issue when attempting to build secure systems *and* while trying to build usable systems. Waiting until the very end to evaluate the result is not the way to achieve security *or* usability.

In contrast, Travis County envisions that their procurement process will result in two performers under contract: a development organization and a "red team" organization. The "red team" will be responsible for attacking the system at every stage of its design and development, ensuring that major architectural problems are discovered and remedied early, when they're cheaper to remedy. We're already doing usability studies on mockups of the system at Rice University which will inform the ultimate designs. Below are two photos of our second-generation prototype ballot box, one showing the voter's experience and another showing the internal paper-handling mechanisms (here, derived from an HP inkjet printer, with the printing parts removed; the whole thing is driven by a Raspberry Pi embedded computer and a variety of cheap accessories, including a laser barcode scanner).



9. The media has made much about the potential of a foreign-nation threat to the 2016 elections, but what about domestic threats: are home-grown hackers also a potential threat for the upcoming elections?

To date, there has been no public evidence of domestic threats of this magnitude. Regardless, foreign nation-state adversaries represent a "worst case" scenario. Any mitigations we might take against foreign adversaries will also protect us against hypothetical domestic threats.

10. Elections typically bring about stories and allegations about one political party trying to manipulate the system in their candidate's favor. Is it conceivable that such action could extend to one part electronically attacking or attempting to hack into voting and election systems to benefit their candidate of choice?

The notable difference between threats abroad and threats domestic is that any analysis of domestic threats must necessarily consider *insider threats*, wherein a poll worker or election official might value their personal partisan preference over their professional non-partisan duty. Generally speaking, when we consider foreign adversaries and their capabilities, we already must consider insider threats, wherein a poll worker or election official might be bribed or otherwise recruited by the foreign adversary.

The main practical impact of insider threats is that we cannot assume that an "airgap" defense is sufficient. A robust voting system must remain robust even in the face of threats from within.

11. In retrospect, has HAVA been a net plus or net minus?

HAVA was a huge benefit to our nation's elections, retiring old and obsolete lever and punchcard systems, and creating the EAC to manage standards and processes. HAVA's greatest failing was disbursing money to purchase new equipment before the EAC and its processes had a chance to even get started. This led us to the present-day situation where expensive equipment, purchased with HAVA, is now aging and obsolete, and was never engineered against an appropriate security model. Sadly, when the EAC tried to add even modest security and other updates to the VVSG requirements, the vendors found the process cumbersome and largely abandoned their products rather than updating them.

As described above (answer to question 8), it's expensive and difficult to add requirements to a complete product, especially when those requirements are best met by changing the entire development process. Conversely, if we had good standards and processes in place *before* the vendors began their work, we'd have equipment that was more usable, more secure, and we

could have made it easier to mix-and-match equipment. Good standards help prevent vendor lock-in, and that in turn, can improve pricing and features in the market.

12. Some experts have stated that the paper ballot is in and of itself secure. Do you agree with that statement?

The best security comes from having *copies* that have different failure modes. A precinct-based optical scanner creates electronic copies of ballots as they are deposited in the ballot box, meaning that post-election stuffing of paper won't be reflected in the electronic records, nor will post-election electronic tampering be reflected in the physical box of paper ballots. An attacker would need to consistently tamper with both paper and electronic records--a significantly harder job than tampering with either one alone. It's worth noting that the security in a scheme like this comes from a *mandatory auditing process*, as part of the post-election "canvass" period prior to the election results being certified. Evidence that's not considered provides no security benefit.

When we envision a sophisticated nation-state adversary engineering custom-built exploits for purposes of attacking an election, we have to consider the very real possibility that all of the electronic records resulting from an election might be tampered. This is where printed paper ballots, *in addition to those electronic records*, provide the strongest possible security model. Once printed, they cannot be "un-printed", particularly if their chain of custody is protected through simple, traditional means (e.g., video cameras, security guards, locked vaults).

The Travis County design, in particular, creates cryptographic "receipts", printed on paper, that voters can take home which allow them to cryptographically *prove* that their ballots were not tampered as part of the tally, while not being able to prove to anybody else how they voted[1]. There are even mechanisms to detect if a machine tried to cheat a voter and record a vote differently from the voter's intent. These sophisticated cryptographic mechanisms work hand-in-hand with printed paper ballots, producing election results that are stronger than cryptography or paper, alone, might accomplish.

[1] We cannot allow voters to take home any sort of receipt that indicates their vote selections, because that would enable bribery and coercion. "Vote for my candidate and I'll pay you $20". When we speak of a "cryptographic receipt", we mean that it prevents this sort of bribery and coercion while still allowing other useful properties to be proven by the voter or by any organization acting on the voter's behalf.

Question submitted by Rep. Eddie Bernice Johnson

1. In response to a recommendation by the Presidential Commission on Election Administration, the CalTech/MIT Voting Technology Project developed a web site that election officials can use to determine if they can deploy a more efficient line management configuration to help shorten lines. The project highlighted the science of line management and queuing theory. What other areas of election and voting science and technology should Congress, particularly this Committee, look to support?

The broad challenge of improving our nation's elections requires not only *secure* voting systems, but also *usable* voting systems. My research involves extensive collaboration with human factors experts to ensure that our security mechanisms don't have a negative impact on voter speed, accuracy, and satisfaction. NIST has a lot of usability expertise, and they've supported some of my colleagues' usability studies on voting. Additional NIST engagement on this issue would be beneficial for studies of all the nuts-and-bolts issues in elections (e.g., poll worker training effectiveness).

Appendix II

Additional Material for the Record

ARTICLE SUBMITTED FOR THE RECORD

The Washington Post

CCH

The Post's View

How to hack- and rig-proof U.S. elections

By Editorial Board August 29 at 7:21 PM

A MONDAY report from Yahoo News's Michael Isikoff raised concerns that this year's election will be rigged — though not in the way Donald Trump has predicted. Election systems in at least two states — Arizona and Illinois — have been compromised, seemingly by foreign hackers, possibly operating out of Russia or Iran. These revelations are only more worrying in light of the Russian government's other apparent attempts to sway this year's presidential election toward Mr. Trump, such as the hacking of the Democratic National Committee and subsequent leaking of party documents.

In fact, for the moment, the news does not suggest that foreign governments are rigging the election, or anything close. Without evidence of deeper penetrations, the latest revelations amount to little more than a warning. Election systems have vulnerabilities. Government officials and perhaps Congress can and should do more to ensure the integrity of the ballot box.

In both states, hackers appear to have been interested in taking rather than changing information stored on state systems, penetrating election databases containing voter information. Even then, they managed to extract information — up to 200,000 voters' personal data — only in the Illinois case. In Arizona, election officials discovered malicious software before any data was taken. Though election tampering might be a motive, the penetrations could have simply been in service of petty crime — hackers gathering personal information to commit identity theft.

U.S. elections are hackable, though it is much harder than some appear to believe. There are three main areas of vulnerability, according to Andrew Appel, a Princeton University computer scientist. Hackers could tamper with voter records, removing names from official rolls. They could attack electronic voting machines. And they could disrupt the proper tallying of voting results as they are collected from various precincts.

In each case, one key to ensuring integrity is creating a paper trail that can be matched to the electronic records. Electronic voter rolls can be checked against paper ones; electronic vote counts can be compared to paper ballots filled in during the voting process; statewide vote tallies can be checked by examining and adding the results reported publicly in each precinct.

Most places have voting machines that leave a checkable paper trail, but there are some counties that do not. Hacking these machines would take some real work — hackers would have to get a virus onto special cartridges used to input election information to the devices — but election officials should consider machines without paper functionality to be unacceptable and replace them as soon as possible.

At the moment, the biggest threat to the integrity of U.S. elections appears to be that politicians, Mr. Trump in particular, will use anecdote and innuendo to stoke a crisis of confidence. Given that Mr. Trump has already indicated he will not accept the legitimacy of an election that ends in his defeat, even a well-functioning electoral system in which any attempted hacks and other frauds are caught and corrected could look to many like a sham. Americans should demand strong electoral safeguards without surrendering to this sort of dangerous cynicism.

Read more:

David Ignatius: Russia's DNC hack: A prelude to intervention in November?

Bruce Schneier: By November, Russian hackers could target voting machines

Ari Berman: Donald Trump is wrong. Rigging an election is almost impossible.

The Post's View: Voters take note: Donald Trump just invited a Russian cyberattack of his opponent

The Post's View: Donald Trump is spinning a loaded electoral conspiracy theory