SECURING AMERICA'S ELECTIONS

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

FRIDAY, SEPTEMBER 27, 2019

Serial No. 116–56

Printed for the use of the Committee on the Judiciary

Available via: *http://judiciary.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE
45–285 WASHINGTON : 2021

COMMITTEE ON THE JUDICIARY

JERROLD NADLER, New York, *Chair*
MARY GAY SCANLON, Pennsylvania, *Vice-Chair*

ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
THEODORE E. DEUTCH, Florida
KAREN BASS, California
CEDRIC L. RICHMOND, Louisiana
HAKEEM S. JEFFRIES, New York
DAVID N. CICILLINE, Rhode Island
ERIC SWALWELL, California
TED LIEU, California
JAMIE RASKIN, Maryland
PRAMILA JAYAPAL, Washington
VAL BUTLER DEMINGS, Florida
J. LUIS CORREA, California
SYLVIA R. GARCIA, Texas
JOE NEGUSE, Colorado
LUCY MCBATH, Georgia
GREG STANTON, Arizona
MADELEINE DEAN, Pennsylvania
DEBBIE MUCARSEL-POWELL, Florida
VERONICA ESCOBAR, Texas

DOUG COLLINS, Georgia, *Ranking Member*
F. JAMES SENSENBRENNER, JR., Wisconsin
STEVE CHABOT, Ohio
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
KEN BUCK, Colorado
JOHN RATCLIFFE, Texas
MARTHA ROBY, Alabama
MATT GAETZ, Florida
MIKE JOHNSON, Louisiana
ANDY BIGGS, Arizona
TOM MCCLINTOCK, California
DEBBIE LESKO, Arizona
GUY RESCHENTHALER, Pennsylvania
BEN CLINE, Virginia
KELLY ARMSTRONG, North Dakota
W. GREGORY STEUBE, Florida

PERRY APELBAUM, *Majority Staff Director & Chief Counsel*
BRENDAN BELAIR, *Minority Staff Director*

C O N T E N T S

FRIDAY, SEPTEMBER 27, 2019

SECURING AMERICA'S ELECTIONS

Friday, September 27, 2019

HOUSE OF REPRESENTATIVES

COMMITTEE ON THE JUDICIARY
Washington, DC

The Committee met, pursuant to call, at 9:05 a.m., in Room 2141, Rayburn House Office Building, Hon. Jerrold Nadler [chairman of the committee] presiding.

Present: Representatives Nadler, Lofgren, Jackson Lee, Cohen, Johnson of Georgia, Deutch, Cicilline, Lieu, Raskin, Jayapal, Demings, Correa, Scanlon, Garcia, Neguse, Stanton, Dean, Mucarsel-Powell, Chabot, Gohmert, Jordan, Buck, Gaetz, Johnson of Louisiana, Reschenthaler, Cline, Armstrong, and Steube.

Staff Present: Aaron Hiller, Deputy Chief Counsel; Arya Hariharan, Deputy Chief Oversight Counsel; Madeline Strasser, Chief Clerk; Moh Sharma, Member Services and Outreach Advisor; Sarah Istel, Oversight Counsel; Julian Gerson, Staff Assistant; Priyanka Mara, Professional Staff Member/Legislative Aide; Matt Robinson, Counsel, Subcommittee on Courts, Intellectual Property, and the Internet; Brendan Belair, Minority Staff Director; Bobby Parmiter, Minority Deputy Staff Director/Chief Counsel; Jon Ferro, Minority Parliamentarian; Ryan Breitenbach, Minority Chief Counsel, National Security; and Erica Barker, Minority Chief Legislative Clerk.

Chairman NADLER. The House Committee on the Judiciary will come to order.

Without objection, the chair is authorized to declare recesses of the Committee at any time.

We welcome everyone to this morning's hearing on "Securing America's Elections."

I will now recognize myself for an opening statement.

Yesterday, the Director of National Intelligence testified that, "the greatest challenge we have as a Nation is making sure to maintain the integrity of our election system." I agree. Our democracy was founded on a government elected by the people, for the people in free and fair elections.

Today, our elections, the very core of our democracy, are under attack. Special Counsel Mueller's report, in no uncertain terms, details how a foreign government attacked our 2016 elections. The Russian objectives were clear: Deepen distrust and discord in our society, secure the election of one candidate for President over the

other, and, in so doing, undermine confidence in the integrity of our elections and damage our Nation's standing in the world.

There is no evidence that Russia affected the actual vote count of our elections, but Russia did successfully steal thousands of documents from American citizens that it used to influence public opinion. It also accessed voter data and gained other valuable intelligence, which it may seek to exploit in the future.

In short, as Special Counsel Mueller emphasized in his recent press conference, Russia's attack, "deserves the attention of every American."

Russia's attack was not an isolated accident, nor is Russia the only foreign power attempting to influence our elections. We live in a world with agile, persistent enemies who are constantly evolving their methods of attack. As FBI Director Christopher Wray warned, "Make no mistake: The threat just keeps escalating. And we're going to have to up our game to stay ahead of it."

Despite concrete evidence confirmed by the heads of our intelligence agencies, President Trump has refused to acknowledge Russia's attack, let alone publicly denounce it, or outline clearly how he intends to deter future interventions. To the contrary, the President has openly declared that he sees no problem with foreign influence in our elections.

More troubling, there have been reports from multiple senior White House officials, including the former Secretary of Homeland Security, the organization tasked with leading our election security efforts, that the White House failed to adequately inform Americans about continuing influence efforts and, instead, directly stymied attempts to investigate or even discuss the attacks on our elections.

More troubling still, we now have evidence that the President of the United States asked a foreign leader to interfere in our next election. The President is not only refusing to defend our elections against foreign attacks but is actively soliciting such intervention.

That is unacceptable, and it puts our Nation at great risk. We must not let foreign attacks go unpunished or undeterred, and we must make the investments necessary to withstand any future attacks.

The Judiciary Committee is tasked with the duty of protecting the right to vote for every American. That includes not just equal voting rights and access to the polls but also confidence in the accuracy and security of our election systems. We will protect that sacred right. We will not let anyone, not even the President, attempt to undermine the integrity of our democracy.

Today's hearing will help carry out that duty to ensure that we understand the extent of the scope and the threat to our 2020 elections and to identify appropriate steps for deterring, detecting, and defending against those threats. I am pleased that the last week the Senate finally approved a bipartisan spending bill to safeguard voting systems, but much more needs to be done.

U.S. elections are not built of isolated parts. The existing infrastructure is a vast ecosystem that includes voter registration, vote-casting, vote tabulation, election-night reporting, and auditing systems. Each of those components is vulnerable to attack. As with

any ecosystem, if any one component part fails, if there is a flaw in one piece of the technology, it can jeopardize the entire process.

As former Secretary of Homeland Security Jeh Johnson explained, the integrity of our election outcomes on a national level dances on the head of a pin. Securing our election system, therefore, requires securing each of its component parts.

This begins with ensuring that we can verify all votes through post-election audits to certify that each vote is accurately counted, which will help maintain trust and transparency in the election process.

We must also secure our voter registration databases, voting machines, and voting systems. A report published this spring found that in at least 40 States voter registration databases and machines were instituted more than a decade ago. Outdated systems are difficult to maintain and are subject to serious flaws and vulnerabilities and are more vulnerable to attacks from the outside.

Our adversaries are agile and technologically advanced. We must be too. We must provide States with the resources needed to secure their systems and update their critical infrastructure.

In addition, nearly all States and territories rely on outside vendors in some capacity, but of those States and territories, roughly 92 percent rely on just three vendors. These vendors must be regulated to ensure that all of their products meet minimum election security requirements.

Finally, State and local officials responsible for administering elections, our democracy's frontline defenders, must have the resources and cybersecurity training necessary to protect our voting systems. We must also develop better tools to share cybersecurity and threat information among State and local officials and the Federal Government.

In 2016, according to the intelligence community, State election officials were not sufficiently warned or prepared to handle an attack from a hostile nation-state actor. We must ensure that each component piece of our election system is sufficiently integrated, equipped, and ready to handle any attack, from any actor, going into 2020 and beyond.

In short, the challenges facing our elections are serious, evolving, and multipronged. There are no easy answers. I know that Ranking Member Collins agrees with me that the threat to our elections is a threat to the American republic.

I thank Mr. Collins for his attention to this issue, and I am pleased to say that our staff jointly selected the witnesses here today. These witnesses will help us understand further the extent and the scope of the threats we face and the vulnerabilities in our systems that must be patched. Their testimony will help guide this committee's efforts to ensure the integrity of our elections, and I thank them for appearing today.

I am confident that, working together, we can address the imminent threat to our elections and protect our voting systems going forward. Our democracy depends on it.

The Ranking Member has been detained, and I will recognize him for his opening statement after he arrives.

Without objection, all other opening statements will be included in the record.

Chairman NADLER. I will now introduce today's witnesses.

Debora Plunkett is a senior fellow for the Defending Digital Democracy Project at the Harvard Kennedy School, Belfer Center for Science and International Affairs, and an adjunct professor of cybersecurity at the University of Maryland Graduate School.

Ms. Plunkett previously served as Deputy Director and then Director of the National Security Agency's Information Assurance Directorate. She also served as a director on the National Security Council under both President Clinton and President George W. Bush.

Ms. Plunkett received a Bachelor of Science degree from Towson University, an MBA from Johns Hopkins University, and a Master of Science in national security strategy from the National War College.

Kathy Boockvar is the acting secretary of the Commonwealth of Pennsylvania. She also serves as the Elections Committee co-chair for the National Association of Secretaries of State and as the association's representative on the Election Infrastructure Subsector Government Coordinating Council. That is a nice title.

Previously, Ms. Boockvar served as senior advisor to the Governor of Pennsylvania on election modernization, as executive director of Lifecycle WomanCare, and as chief counsel for the Pennsylvania auditor general. Ms. Boockvar also worked for many years as a poll worker and voting rights attorney.

Ms. Boockvar received a Bachelor of Arts degree from the University of Pennsylvania and a J.D. from American University Washington College of Law.

Mr. RASKIN. Will the gentleman yield?

Chairman NADLER. I yield to the gentleman.

Mr. RASKIN. She was my student.

I yield back.

Chairman NADLER. I will assume she learned well.

Tom Burt is the corporate vice President of the Customer Security and Trust Team at Microsoft Corporation, where he works to formulate and to advocate Microsoft's cybersecurity policy globally, including advancing the Digital Geneva Convention, the Tech Accord, and the Defending Democracy Project.

Mr. Burt joined Microsoft in 1995 and has since held several leadership roles in the Corporate, External, and Legal Affairs Department, including leading the company's litigation group from 1996 to 2007 and, more recently, leading their Digital Trust team.

Prior to joining Microsoft, Mr. Burt was a litigation partner at Riddell Williams, a law firm in Seattle, where he worked on voting rights cases.

Mr. Burt received a Bachelor of Arts degree from Stanford University and a J.D. from the University of Washington Law School, where he graduated magna cum laude.

We welcome all our distinguished witnesses, and we thank them for participating in today's hearing.

Now, if you would please rise, I will begin by swearing you in. Raise your right hands, please.

Do you swear or affirm under penalty of perjury that the testimony you're about to give is true and correct to the best of your knowledge, information, and belief, so help you God?

Thank you.

Let the record show the witnesses answered in the affirmative.

Thank you, and please be seated.

Please note that each of your written statements will be entered into the record in its entirety. Accordingly, I ask that you summarize your testimony in 5 minutes. To help you stay within that time, there is a timing light on your table. When the light switches from green to yellow, you have 1 minute to conclude your testimony. When the light turns red, it signals your 5 minutes have expired.

Ms. Plunkett, you may begin.

TESTIMONY OF DEBORA PLUNKETT

Ms. PLUNKETT. Chairman Nadler, Ranking Member Collins, and distinguished Members of the committee, thank you for the opportunity to testify before you today.

My testimony focuses on potential security vulnerabilities of our election systems and recommendations to better protect our democratic processes and systems from cyber attacks.

We must take bold, decisive, and expeditious steps to address cyber threats and then assume our efforts are insufficient given the rise of attackers' capabilities. All known threats must be addressed in order to better ensure secure and trusted elections.

Bad actors, whether nation-states or lone criminals, focus on gaining unauthorized access to systems that provide the best opportunity to achieve their goals, including influence, destruction, profit, espionage, coercion, or just fun and fame. Attackers can make their attempts from across an ocean or from down the street.

We must treat election security as imperative for safeguarding our democracy. Intelligence leaders warn of ongoing and escalating interference attempts by multiple foreign actors who view our 2020 elections as an opportunity to advance their interests at the expense of American democracy.

In the United States, elections are complex and decentralized. The United States has over 10,000 election jurisdictions. These jurisdictions vary by technology and processes. Recognizing the variety of election jurisdictions is central to developing and implementing strategies to improve election infrastructure security.

While elections operations can vary significantly across jurisdictions, there are fundamental similarities in some infrastructures. Many election systems are built using general-purpose technology and commercial off-the-shelf software. While this means they are often subject to attacks popular in other sectors, it also means experts have identified some best practices to mitigate many of the risks. The key is to make sure these solutions are kept up to date.

At Harvard, the Belfer Center's Defending Digital Democracy Project produced a State and local elections security playbook which identifies 10 best practices that apply to all elections' jurisdictions, which I'll briefly summarize today.

The first is to create a proactive security culture. Most cyber compromises start with human error. A strong security culture makes a big difference as to the success of a malicious actor.

The second is to treat elections as an interconnected system. Any digital device that touches election processes must be safeguarded. Device security management should be centralized and streamlined.

The third is to require a paper vote record. It is essential to have a voter-verified, auditable paper record to allow votes to be cross-checked against electronic results. The paper record must have a rigorous chain of custody.

The fourth is to use audits to show transparency and maintain trust in the elections process. Auditing should be embedded at points in the process where data, integrity, and accuracy are critical.

The fifth is to implement strong passwords and two-factor authentication. While strong passwords are important, two-factor authentication is one of the best defenses against account compromise.

Number six is to control and actively manage access, where users should receive the minimum access required to perform their jobs. When someone no longer needs access, it should be revoked.

Number seven is to prioritize and isolate sensitive data and systems so that you know which systems should be properly protected.

Number eight is to monitor, log, and back up data, which enables attack detection and system or data recovery after an incident.

Number nine is to require vendors to make security a priority. Detailed security specifications should be written into acquisition documents, and vendors must be required to notify officials immediately after becoming aware of a breach.

Finally, number 10 is to build public trust and prepare for information operations. Transparency and open communications will counter information operations that seek to cast doubt over the integrity of the election system.

In conclusion, election systems are critical infrastructure. To protect them, the Federal Government must provide the requisite guidance and support by allocating resources to upgrade election systems to the highest security standards; ensuring information exchange between Federal, State, and local entities is seamless; instituting security standards that vendors must follow for election systems or components; and encouraging a culture of security by keeping the American public fully informed on malicious actors' behaviors and intentions and the government's efforts to stop them.

Thank you for the opportunity to participate in this important dialogue today.

[The statement of Ms. Plunkett follows:]

7

Debora A. Plunkett

Senior Fellow, Belfer Center, Harvard University

September 27, 2019

U.S. House of Representatives Committee on the Judiciary

Hearing: "Security America's Elections"

Written testimony of Debora A. Plunkett, Senior Fellow, Defending Digital Democracy, Belfer Center, Harvard University for the hearing of the U.S. House of Representatives Committee on the Judiciary titled "Securing America's Elections"

Friday, September 27, 2019 9:00 AM

Chairman Nadler, Ranking Member Collins and Distinguished Members of the Committee, thank you for the opportunity to testify before you today to discuss potential security vulnerabilities of our election systems and political campaigns, and solutions to mitigate those vulnerabilities.

My testimony today will focus on identifying and recommending solutions to protect democratic processes and systems from cyber and information attacks. Concrete solutions are needed to address this urgent problem. Foreign nations and non-state actors are not backing down in their efforts to hack systems, alter the outcome, and undermine confidence in our elections.

Our democracy is under attack and at risk. Threats to elections is a national security issue. We must take bold, decisive and expeditious steps to address them, and then assume that they are insufficient given the rise of nation state capabilities and intentions, and the relative known insecurities of elections systems. Threats to campaigns and candidates is also of grave concern as malicious actors have discovered and are exploiting weaknesses in the communications and technology security for candidates. Finally, there are almost certainly election system weaknesses that either have yet to be discovered or even vulnerabilities that have yet to be created, reinforcing the need for constant monitoring. All of these threats must be addressed in order to insure secure and trusted U.S. election processes.

Our elections are under attack

A core tenet of our democracy is that the government reflects the will of the people. Elections are the quintessential expression of this principle and citizens won't trust their government unless they trust the election process and the integrity of its outcome.

Perception is reality. An adversary can manipulate the outcome of an election through actual cyber operations, but they can get the same result (i.e., erode trust in the process) by using information operations to make the public *believe* that the election was manipulated, even if it was not in reality. The U.S. intelligence community reported that cyber and information operations took place in the 2016 presidential election. These malicious acts revealed significant vulnerabilities in our elections process. "Russian interference operations against the United States during the 2016 presidential election were vast and complex. That's the conclusion drawn by Special Counsel Mueller, as well as by the Department of Justice, the Intelligence Community, and the Senate Select Committee on Intelligence, in the course of their respective investigations. The Russian government waged a well-documented, sustained campaign to weaken the United States, using multiple tools and tactics, damage our democracy and divide our citizens. That campaign continues today." According to the Department of Homeland Security (DHS), Russia targeted the election infrastructure of 21 U.S. states in advance of the 2016 election and were successful at penetrating a small number of them.

The 2016 election interference was not the first-time malicious actors have meddled with U.S. elections, and it will not be the last. In January 2018, the Director of the Central Intelligence

Agency, Mike Pompeo, stated he has "every expectation" Russia will continue meddling in U.S. elections. This proved true during the 2018 midterm elections, where press reporting indicates that Russia used internet trolls and bots to launch and promulgate disinformation through ads on social media platforms. An October 2018 Department of Justice indictment stated that from December 2014 until at least May 2018, Russian military intelligence officer "conducted persistent and sophisticated computer intrusions affecting U.S. persons, corporate entities, international organizations, and their respective employees located around the world, based on their strategic interest to the Russian government."

Bad actors, whether nation states or criminals, focus on gaining unauthorized access to those systems that provide the best opportunity to achieve their individual interests, whether it be for influence, destruction, profit, espionage, coercion and just fun and fame. Regardless, in order to protect that for which our nation was created, we must focus on election security as an imperative for safeguarding our democracy. Intelligence leaders warn of ongoing and escalating interference attempts by multiple, foreign actors who view our 2020 elections as an opportunity to advance their interests at the expense of American democracy.

A range of adversaries have both the capability and intent to inflict harm on the democratic process using cyber and information operations tools. They can do this from an ocean away or right down the street. The Russian intelligence services partially achieved President Putin's goal of undermining trust in American democracy by using a combination of cyber attacks and information operations to influence narratives of the 2016 presidential election. This partial success, and the U.S. government's failure to respond sufficiently to the Russians, likely means that future elections will face attack from a broader set of actors. Nation-states pose the most well-resourced and persistent threat. Lone "black hat" hackers and cybercriminals, who may be motivated by personal gain, notoriety, or the simple desire to see if they can succeed, are also a salient threat.

Russia is not our only threat. In the 2008 and 2012 U.S. presidential elections, Chinese hackers are believed to have penetrated Democratic and Republican presidential campaigns. These breaches appear to have been focused on intelligence gathering as there is no evidence hackers released stolen materials or attempted to interfere with state election systems. In 2016, the U.S. Justice Department identified Iran as the culprit in a 2013 cyber attack against a small piece of U.S. physical infrastructure, as well as a series of denial of service attacks on major U.S. financial institutions. Iran demonstrated strong cyber operational capabilities during its penetration of U.S. Navy unclassified networks in 2013. As geopolitical tensions with Iran rise, Iran's cyberspace capabilities could pose a future threat to U.S. elections.

Finally, while there is no evidence to date of North Korean election-related hacking, the regime has targeted other industries. North Korean hackers infamously retaliated against Sony Pictures Entertainment for producing the film "The Interview" by stealing and releasing company emails and wiping out large parts of Sony's information systems. The U.S. government has attributed the "WannaCry" campaign, which damaged computers across the world, including the U.K. The National Health Service, to North Korea. Additionally, government-linked hackers have conducted a series of cyber attacks on financial institutions, central banks, and the global SWIFT financial transaction system, with the aim of raising money for the regime. Heightening tensions

between North Korea and the U.S. could provide North Korea with incentive to undermine American democracy, and prompt future attacks.

Elections are administered by diverse localities

U.S. elections are decentralized and are administered by the states. The federal government provides national-level guidance, but state and local governments oversee elections. In almost every state, local officials at the county or municipal level have direct responsibility for the conduct of elections in jurisdictions ranging in size from a few dozen to nearly eight million eligible voters. The distributed and decentralized nature of elections is both good and bad for cybersecurity. Fortunately, decentralization makes it hard, though not impossible, for a single cyber operation to compromise multiple jurisdictions. However, disparities in cybersecurity resources and experience across jurisdictions creates vulnerabilities. Smaller jurisdictions with fewer resources may be seen as more vulnerable targets by adversaries. The Belfer Center's Defending Digital Democracy project conducted a nationwide security survey of states and territories, finding that the most frequent concern noted by election officials was insufficient resources to secure the process, especially in smaller counties.

It is difficult to defend the multifaceted nature of the elections processes. In the United States, elections are among the most complex and decentralized operations in either the public or private sectors. Every state and locality is unique, with various intricacies in election operations. According to the National Conference of State Legislatures, the United States has over 10,000 election administration jurisdictions. These jurisdictions vary greatly in the number of voters they serve, number of personnel they employ, election infrastructure in use, cybersecurity resources at their disposal and organizational structure of election administration ownership. Additionally, these jurisdictions are relatively autonomous and have varied plans for the future of election administration under their purview. Recognizing the variety of election jurisdictions is central to developing and implementing strategies aimed at improving election infrastructure security.

Elections systems use general purpose applications

While the qualities of jurisdictions can vary significantly, there are fundamental similarities for infrastructures. Many election systems are built using general purpose technology and commercial-off-the-shelf software. While this means they are often subject to attacks popular in other sectors, it also means experts have identified best practices to mitigate many of the risks. Therefore, for many components of election infrastructure best practices for mitigating risks are largely similar to general IT security best practices.

Components of Election Systems

Election systems and components generally can be categorized into three levels of operation relating to cybersecurity risk. Officials in all jurisdictions, regardless of size, must secure the process at each level. The first level includes the core systems that make elections run: voter registration databases (VRDBs), electronic poll books, vote capture devices, vote tally systems, and election night reporting (ENR) systems. The second level includes two intermediary government functions that connect to multiple election system components: other state and county-level systems, and election officials' internal communication channels. Finally, the third level involves external functions that touch the entirety of the elections process: vendors, and traditional and social media at the local and national level.

Voter Registration Databases and Pollbooks

Voter registration systems provide voters with the opportunity to establish their eligibility and right to vote, and for states and local jurisdictions to maintain each voter's record, often including assigning voters to the correct polling location. These are typically network connected databases. The inputs to voter registration databases (VRDBs) are registrations, removals due to ineligibility (e.g., an individual moving out of state, death of a voter), and record updates, most often due to an individual moving within the state. The outputs include facilitating retrieving voter information —such as a voter verifying, they are registered, seeking a sample ballot, or finding their polling place—and transfer of voter information to pollbooks. The most common method of voter registration is through a states' DMV.

Pollbooks provide voter registration information to workers at each polling location. They are necessary to ensure voters are registered and are appearing at the correct polling place, and pollbooks being used efficiently is necessary to limit voters' wait times. Pollbooks can take the form of preprinted paper registration lists or as an electronically accessed database, known as an e-pollbook. About 48 percent of voters who cast ballots in person in 2016 were signed in at the polls by election workers using e-poll books, compared to only 27 percent in 2012.

Attacks on VRDBs and e-pollbooks could result in individuals being incorrectly allowed or denied the right to vote. These attacks could also result in confusion at the polls, undermining confidence in the integrity of elections.

Vote Capture Devices

Vote capture devices are the means by which individuals' votes are cast and recorded - the voting machines. As with other election technology, machines and process for vote capture vary by jurisdiction. Furthermore, any given jurisdiction, and even a single polling place, is likely to have multiple methods for vote capture to accommodate administrative decisions and voters with varied needs or preferences. For example, on election day, a polling place may give voters the choice of voting using an electronic voting machine or a paper ballot. Another instance, voters with language needs or voters with disabilities may necessitate the use of additional components or a separate device.

The 2000 recount in Florida exposed significant limitations with punch card voting machines, which accounted for 30% of vote capture machines at the time. In 2002, Congress passed the Help America Vote Act (HAVA) which included $3 billion of funding for states to revamp their voting technology. With this funding, voting machines were replaced wholesale with more and more jurisdictions adopting mostly or purely electronic machines.

The new purely electronic machines spurred controversies of their own around whether they could be trusted to record and report votes accurately. Additionally, by the mid-2010s most of these machines had become obsolete and in 2014 the Presidential Commission on elections warned there was an "impending crisis" in voting technology. As of 2016, most of the HAVA funds that were distributed to states for the purpose of refreshing their voting technology had been exhausted. 65% states and territories in the US have less than 10% of their originally allocated HAVA funds left, another 14 states and territories (25%) had less than half of their funding left.

The Consolidated Appropriations Act of 2018 included $380 million in additional funding for election security in conjunction with the HAVA act. According to the EAC, 100% of new HAVA funds were disbursed by Sept 20, 2018. The EAC believes as of April 30, 2019, states have spent at least $108.14 million, or 29 percent of the $380 million in grant funds. A straight-line spending projection based on expenditures through the end of March 2018 suggests that states and territories will spend approximately $324 million, or 85 percent, of the funds prior to the 2020 Presidential Election. States plan to use about 28% of these funds on voting equipment.

On June 26, 2019 the House passed its FY2020 Financial Services and General Government appropriations bill which included $600 million in additional HAVA funds to be distributed to states for election security. On September 19, 2019 the Senate Appropriations Committee voted to advance its FY2020 bill which only includes $250 million for HAVA funds to be distributed to states for election security.

According to the Brennan Center for Justice, a minimum investment of $2.153 billion over the next five years is necessary to "bring all states to a reasonable baseline on election security." Contained within that estimate, is $734 million for replacing machines older than 10 years and to replace direct-recording electronic (DRE) voting machines which do not provide a paper record.

Best Practices for Securing Election Systems
The Belfer Center's State and Local Election Cybersecurity Playbook identifies ten best practices that apply to all election jurisdictions, specifically:

1. **Create a proactive security culture**. Risk mitigation starts with strong leaders who encourage staff to take all aspects of election security seriously. Most technical compromises start with human error—a strong security culture can help prevent that. A strong security culture also makes a big difference as to whether a malicious actor: (1) chooses to target an organization, (2) is able to successfully do so, or (3) is able to create a public perception that the organization has been compromised. Any state could experience a cybersecurity threat to their elections process—it is the job of leaders to make sure they are prepared. Senior election officials must lead by example, issuing guidance about the necessity of applying cybersecurity standards, stressing the importance of cybersecurity for staff and following up with operations personnel regarding the implementation of improved cybersecurity protections. Developing a detailed cyber incident response plan and mandating frequent testing of critical systems will ensure both resilience and comfort with crisis management. There is a wealth of expertise available to support improving cyber defense capabilities. Election officials should leverage these resources to complement their in-house expertise. Finally, election officials must be diligent in selecting those who will be involved in election administration. Background checks should be conducted on all personnel accessing sensitive information and privileged systems, and vendors should be required to do the same.

2. **Treat elections as an interconnected system**. Adversaries can target not only individual parts of the election process but also the connections between them. Attackers look for

seams: they seek the weakest point and move from three to their intended target. External systems (e.g., Department of Motor Vehicles databases and vendors) with election system access must be included in the system landscape because they can be penetrated to gain access. The compromise of one part of the election system or an external source can potentially corrupt seemingly unrelated parts of the system. This is true even if the system is not technically connected to the Internet because attacks can be executed using mobile storage devices (e.g., thumb drives) or other external storage devices. Any computer or other digital device that touches election processes must be safeguarded. Device security management should be centralized and streamlined by incorporating election offices into existing technology security plans.

3. **Require a paper vote record**. To protect against cyber attacks or technology failures that could jeopardize an election, it is essential to have a voter-verified auditable paper record to allow votes to be cross-checked against electronic results. Without a paper vote record, accuracy and integrity of the recorded vote tally depends completely on the correctness and security of the machine's hardware, software and data; every aspect from the ballot displayed to the voter to the recording and reporting of the votes, is under the control of hardware and software. Any security vulnerability in this hardware or software, or any ability for an attacker to alter (or reload new and maliciously behaving) software running on a machine that does not produce a paper record, not only has the potential to alter the vote tally but can also make it impossible to conduct a meaningful audit or recount (or event to detect that an attack has occurred) after the fact. As a result, an auditable paper record must be created for every vote cast that is verified by the voter and the paper record must have a rigorous chain of custody associated with it.

4. **Use audits to show transparency and maintain trust in the elections process.** Audits are a mechanism to detect intrusions or manipulations on electronic systems that may go unnoticed and reassure the public that the elections process works. This is an important part of the public engagement strategy that builds confidence and demonstrates transparency. *When combined with #3, having an auditable paper vote record, this substantially reduces the risk of a malicious actor delegitimizing an election.* Auditing should be embedded at points in the process where data integrity and accuracy are critical; for example, with voter registration records. Post-election audits should be standard practice, using paper records to confirm electronic results

5. **Implement strong passwords and two-factor authentication.** Malicious actors frequently use stolen user credentials (e.g., username and password) to infiltrate networks. Although strong passwords are important, *two-factor authentication is one of the best defenses* against account compromise. Two-factor authentication typically requires a user to present something they *know* (a username/password) and something they *have* (such as another associated device or token) in order to access a digital account. Only by having *both of* these things will the user confirm their identity and be able to gain access to the system. Strong passwords must be required not only for official accounts but also for key officials' private email and social media accounts.
6. **Control and actively manager access.** Everyone with access to the computer network can become a target and often only one target needs to be compromised for an attack to

succeed. The more people who can use a system, and the broader their access rights, the greater the opportunities for malicious actors to steal credentials and exploit them. As a result, there should be a limit on the number of people with access to the system with a focus on providing access to those who need it to complete their jobs. Additionally, using the principle of 'least privilege' will restrict what each user is authorized to do, giving the minimal level of access required to perform their jobs. Finally, anyone who no longer needs access, regardless of their privilege level, should be quickly removed from access. This should be a standard offboarding procedure.

7. **Prioritize and isolate sensitive data and systems.** Risk is where threats and vulnerabilities meet. To reduce risk, officials need to think about what vulnerabilities will cause the most damage, given the threat environment. Officials should consider two things when making a risk assessment: (1) what data is most sensitive and (2) what disruption could be most damaging to voters' trust in the election. They should then prioritize mitigating the vulnerabilities that could lead to this damage by isolating and protecting these systems first. Every part of the system is important, but a good security strategy will determine which systems are most sensitive and prioritize efforts there, since these extra protections create operational hurdles and increase costs. Devices with sensitive data should be configured to only be used for their specific purpose in the elections process, and the use of removable media devices (e.g. USB/thumb drives) should be restricted and carefully monitored.

8. **Monitor, log and back up data**. Monitoring, logging, and backing up data enables attack detection and system or data recovery after an incident. When it comes to monitoring, a combination of human and technical means is best. Local officials highly knowledgeable about their jurisdictions can identify many irregularities. However, this alone may leave gaps in detecting attacks. Automated forms of data monitoring, especially at the state level to detect cross country patterns, are critical for detecting anomalies and highlighting when manipulation or intrusion occurs. Backups should be regularly performed, should be read-only once to prevent data corruption, and should be regularly tested by performing a complete restoration from backups. Backups should also be stored in a different physical location than the master database and should be physically secured.

9. **Require vendors to make security a priority**. Vendors design and maintain hardware and software that affect voter registration, vote capture and tallying, electronic pollbooks, election night reporting, and public communication. A Belfer Center study found that 97% of states and territories used a vendor in some capacity. Some vendors service multiple states— meaning an attack on one vendor could affect many elections. Conversely, smaller vendors may not dedicate the necessary resources to cybersecurity, making them unable to defend against sophisticated attacks. Specific and explicit security specifications and standards should be written into contract proposals, acquisition documents and maintenance contracts to ensure that vendors follow sufficient security standards and guarantee state and local governments' ability to test systems and software. Vendor security commitments should be independently verified and periodically tested. Finally, vendors must be required to provide notification of any system breach immediately after they become aware of it.

10. **Build public trust and prepare for information operations.** Communication is the cornerstone of public trust. Transparency and open communication will counter information operations that seek to cast doubt over the integrity of the election system. Communicate with the public to reinforce the message that integrity is a top priority. Start informing the public about cybersecurity threats before elections are held. Include the steps taken to counter the threats and readiness to respond in the event of an attack. Establish processes and communications materials to respond confidently and competently in the event of an attack. Build relationships with reports, influencers and key stakeholders to establish trust and have good communications channels before an incident occurs. Finally, routinely monitor social media, email accounts, and official websites and establish points of contact with social media firms.

Conclusion

To protect our election systems, it is imperative that we prepare, protect and persist. In preparation, we create a culture of security by establishing clear ground rules from the top down, discuss security policies with those who have access to systems, and minimize any weaknesses in people, processes, or technology. Protect involves building resilience by instituting the strongest defenses that can be afforded, and then ensuring a layered approach to security to minimize the potential for easy access with little effort. Finally, persistence is all about vigilance. Developing plans ahead of time, practicing them before game day, and reviewing the plans after implementation are critical steps. Adversaries are diligent, too!

Election systems must be treated as critical infrastructure. This means that there must be appropriate levels of investment. Also, there must be mechanisms for collaboration among states/local jurisdictions with established information sharing channels. Additionally, there is a need for process(es) to share and act on critical threats; checks and balances on appropriate installation of equipment; requirements for vendors to deliver systems free of known vulnerabilities, and to meet specific security standards (back-ups, software assurance, etc.).

Finally, the Federal Government must provide requisite support for elections by allocating resources to upgrade election systems to the highest security standards; insuring information exchanges between federal, state and local entities is seamless, timely and relevant; instituting security standards that vendors must follow for election systems or components used for such systems; and enforcing a culture of security by acknowledging the threat and keeping the American public fully informed on malicious actors, intentions and the government's efforts to eradicate them.

Chairman NADLER. Thank you.
Ms. Boockvar?

TESTIMONY OF KATHRYN BOOCKVAR

Ms. BOOCKVAR. Chairman Nadler and esteemed Members of the committee, thank you so much for your leadership on election security.

As chief election official of Pennsylvania, I have the privilege of working with dedicated election officials across the Commonwealth, in all 67 counties, to make sure that all of our elections are fair, accessible, and secure for all eligible voters.

As has already been discussed, the issues surrounding election Administration have become more complex and complicated because of security issues. As we know, foreign adversaries are continuously trying to influence our elections. The key to thwarting this effort is to make sure that we are building our cyber walls faster than those that are trying to tear them down.

Election security is a race without a finish line, and our adversaries are not slowing down. We need to make sure that we are meeting and exceeding those technologies and making sure that we invest, at all levels, substantial and sustained resources.

Alongside the great majority of States, we urge the Federal Government to provide additional election security funding but also infrastructure.

We need to look at this like we look at other ongoing initiatives. So, we don't do once-and-done appropriations for other types of security, for healthcare, for education. We look at these as ongoing investments, and that's how we have to look at our elections. Nothing is more important than the security of our democracy.

There have been great advances over the last many years. As discussed, the EIS–GCC, the Election Infrastructure Subsector Government Coordinating Council—say that five times fast—has been a great collaboration among Federal, State, and local officials to secure elections. It's working to formalize and improve information-sharing, communication protocols, to make sure that our local and State election officials can respond timely to threats.

The great thing about EIS–GCC is that it has a wide range of Members. So, we've got 29 Members; 24 of them are local and State election officials. But, it also includes critical Federal partners like DHS, EAC, NASED, the Election Center, and the International Association of Government Officials.

Other key partners in this fight are DHS, National Guard, and Center for Internet Security, who have been incredibly strong partners, making sure that we have risk and vulnerability assessments, shared intelligence, tabletop exercises, and extensive communications.

There's more that we could do. So, one of the things that I'd love to see the Federal Government being more involved in is vendor oversight, tracking foreign ownership, making sure that we're getting background checks, making sure that there's a good chain of custody across all voting and election components.

We also need to strengthen lines of communication in both directions from Federal, State, and local. For example, when there are local incidents reported to our Federal partners, the Federal part-

ners need to make sure that the State election officials know so that we could timely respond to those incidents.

On the Pennsylvania landscape, we've had some great successes over the last year and a half that I've been very proud to be a part of. We've really had a very—we broke down silos. We knew it was really important to have an integrated approach to election security. It's been incredibly effective.

We have an interagency workgroup that involves IT professionals, security, law enforcement, homeland security, elections, and emergency preparedness. We meet regularly and work together to make sure that we are working together as a front to make sure we have the most secure and accessible elections in Pennsylvania.

We've provided tabletop exercises, and we were the first State in the country to accept DHS's offer of free vulnerability assessments to States.

One of our big successes over the last year has been our transition in Pennsylvania to voter-verified paper ballot systems. I'm happy to say that, whereas a year ago we had 50 counties across Pennsylvania that had no paper trails, as of this November there will be 52 counties that will have voter-verifiable paper trails. So, a huge flip, great success. The credits to the county election officials for all their work.

I'm also happy to say that we have a post-election audit workgroup, as discussed by Chairman. This is a critical piece of our elections, is making sure that we're auditing and instilling confidence in our voters about confirming the results of the election.

The right to vote is a fundamental right, and every voter must be provided equal access to polls and a deep-seated confidence in the security and accuracy of their votes. Our democracy and bolstering our confidence in that democracy is worth every dollar.

Thank you very much.

[The statement of Ms. Boockvar follows:]

COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF STATE

Testimony of Kathy Boockvar
Acting Secretary of the Commonwealth
Commonwealth of Pennsylvania
Hearing on *Securing America's Elections*
U.S. House of Representatives, Committee on the Judiciary
September 27, 2019

Chairman Nadler, Ranking Member Collins, and distinguished members of the House Judiciary Committee, my name is Kathy Boockvar, and I am the acting Secretary of State (or Secretary of the Commonwealth) of Pennsylvania. As Secretary, I lead the Pennsylvania Department of State (DOS) to promote the integrity and security of the electoral process, protect public health and safety by licensing professionals, support economic and nonprofit development through corporate and charitable registrations, and sanction professional boxing, kick-boxing, wrestling and mixed martial arts. Prior to being appointed as Secretary, I served as Senior Advisor to Governor Wolf on Election Modernization, leading and managing initiatives to improve security and technology in Pennsylvania's elections, in collaboration with federal, state, and county officials.

Thank you for inviting me to testify at your *Securing America's Elections* hearing. As the Chief Election Official of Pennsylvania I have the immense privilege of working with extraordinarily dedicated election directors and personnel in all 67 counties across the Commonwealth, as well as committed Secretaries of State across our great nation, to ensure that our elections - elections that allow candidates running for every local, state, and federal office to serve – are free, fair, secure, and accessible to all eligible voters. In August 2019, I was also honored to be asked to serve as the Elections Committee Co-Chair for the National Association of Secretaries of State (NASS).

The issues surrounding security have made election administration more challenging and complex than ever. As we have learned over the last several years, foreign adversaries and other cyber actors have attempted and continue to attempt to influence elections in the United States. The key to thwarting this effort is that we must continue to build and strengthen our walls faster than those that are trying to tear them down. Election security is a race without a finish line, and our adversaries are continuously advancing their technologies. We must do the same and more; our success is dependent on substantial and sustained dedication of resources.

Alongside the great majority of states across the nation, we urge the federal government to provide additional election security funding and support to counties and states and reinforce our collective infrastructure. All of us at the federal, state, and local levels benefit from the security of our elections, so funding these critical operations must be a cost-share by the federal, state, and local levels. Because the technologies and attempted attacks are becoming more

SECRETARY OF THE COMMONWEALTH
302 North Office Building | 401 North Street | Harrisburg, PA 17120-0500 | 717.787.6458 | Fax 717.787.1734 | dos.pa.gov

sophisticated all the time, we need to plan for and invest in election security like we invest in other ongoing initiatives and challenges. Like other types of security, like STEM fields, like education of our children – investment cannot be once and done, and it should never be dependent on political winds. There is nothing partisan about ensuring that our elections are secure and accessible to all eligible voters. We must have a continuous investment in election security at all levels, both in funding and in strengthening our infrastructure, communications, and responsiveness, so that we may advance and adapt to change as new information is gained and new technologies advanced.

NATIONAL LANDSCAPE

There have been some great advances in election security over the last several years at all levels, while challenges continue to emerge as well. All these – continuing to strengthen advances and pursuing additional goals forward - require significant funding, proactive bi-partisan leadership, quick response time, multi-agency collaboration, and other support.

The National Association of Secretaries of State (NASS), National Association of State Election Directors (NASED) and Secretaries and election officials across the country have been resolute in our commitment to bolstering security in elections, and collaboration at all levels. As NASS Elections Committee Co-Chair, I look forward to working with my fellow Co-Chair Secretary Mac Warner (W.Va.) and with colleagues across the country, to share best practices and provide the most secure and accessible elections to eligible voters in Pennsylvania and nationwide. One of my responsibilities as Co-Chair is to serve as a NASS representative on the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC).

In January 2017, when the federal government designated election infrastructure as part of the nation's critical infrastructure, the EIS-GCC was one of the first developments of that designation. The EIS-GCC is a first of its kind collaboration among federal, state, and local officials to secure elections, working to formalize and improve information-sharing and communication protocols to ensure that timely threat information, support, and resources reach all election officials so they can respond to threats as they emerge. The EIS-GCC has 29 members, of which 24 are state and local election officials. It also includes members from the U.S. Department of Homeland Security (DHS), the U.S. Election Assistance Commission, the National Association of State Election Directors (NASED), the Election Center, and the International Association of Government Officials. The members of the EIS-GCC are working to update an elections-sector specific plan, improve communications protocols and portals, and secure increased resources for state and local election officials. In addition to the GCC, a Sector Coordinating Council (SCC) was also established for non-government, private sector entities to better communicate with election officials and the federal government.

Beyond the EIS-GCC, DHS and the Center for Internet Security (CIS) have been particularly strong partners. Pennsylvania and other states regularly collaborate with DHS on independent risk and vulnerability assessments, intelligence, training, tabletop exercises, communications,

and more. We also work with CIS's Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and Analysis Center, (EI-ISAC) to gather and share intelligence about cyber threats that target government or government-affiliated systems, and gain support and resources including forensic analyses and emergency response assistance. Additionally, the cyber defense team of the Pennsylvania National Guard has been an exceptionally strong partner. Within the last year they were the first National Guard team selected to participate in a new DHS program, to be trained to conduct Risk and Vulnerability Assessments to DHS standards.

For all these strong collaborative partnerships to be most effective, and for additional goals to be advanced, more resources are needed. Some top priorities would include the federal government playing a greater role with vendor oversight, including tracking vendor foreign ownership, data hosting, manufacturing and employee background checks, and chain of custody for all voting and election system components; and reinforcing Continuity of Operations Plans (COOP) across levels and sectors, to provide more clarity on primary points of contact in the federal government for incidents and concerns. It would also be beneficial to have broader communications between our federal election security partners and our state legislatures and counties, so that counties and legislators could hear directly about federal election security priorities and concerns. We also need to strengthen lines of communication from the federal government to the state chief election officials, for example to ensure that federal entities notify the state when local incidents are reported, so that we may immediately act when necessary. Additionally, federal funding and support are needed to ensure that all counties have state-of-the-art intrusion detection systems, comprehensive phishing, cyber hygiene, and security awareness training, vulnerability assessments, and more.

PENNSYLVANIA LANDSCAPE

Most people have an understanding that the word "cyber" relates to the study of systems and the intersections and communications between people and machines. But the word "cyber" actually has ancient Greek origins, deriving from the Greek word for the "gift of governance" and "leadership." In Pennsylvania, we have been tapping both aspects of the word in our election security planning, using resilient and integrated governance and leadership to enhance the intersections and communications between people and machines, to continue to advance our technologies while also doing so in a way that protects our democracy and develops collaborative and responsive policy and leadership. This requires a tremendous amount of resources but has immeasurable value.

Collaboration

Thanks to Governor Wolf's deep commitment, we have employed a multi-layered and cross-sector security strategy to election security. We broke down silos and brought together experts from multiple fields and sectors at the local, state, and federal levels, including professionals in information technology, law enforcement, homeland security, defense, elections, and emergency preparedness. Beginning in 2018, we formed an executive Interagency Workgroup on Election

Security and Preparedness, banding together experts from the Department of State (DOS), Homeland Security, Emergency Management Agency, Information Technology, State Police, National Guard, the Inspector General, and the Department of Military and Veterans Affairs. This team of key agencies meets regularly and collaborates on increasing election security training, support, assessment, information, and preparedness, to implement best practices to respond to and mitigate continuously evolving security threats.

We also formed a county/state election security workgroup of County Commissioners Association of Pennsylvania (CCAP), county election directors, DOS staff, and county and state CIOs and IT personnel. This workgroup discusses security issues and shares training resources, including guidance, security awareness training, and resources on strong cyber security practices for voting system and network preparation and security, including pre-election testing, password and permissions management, restricting access, file transfers, and vote canvassing. We are also providing anti-phishing and security training tools to all 67 counties at no cost to them.

We have collaborated with all these state and federal partners to provide tabletop exercises to counties and partners, modeled after common military and law enforcement techniques, to train election, information technology, and security personnel in incident response and preparation, simulating scenarios that could impact voting operations.

We were the first state in the nation to accept DHS's offer to provide vulnerability assessments to the states – we did this in 2016, 2018, and are planning a third assessment in the next several months. We have tools in place to identify vulnerabilities, detect network intrusion, and encrypt data in-transit and at rest. We engage in ongoing continuity and disaster recovery exercises and review and revise as necessary our COOP plans several times each year.

Voting System Upgrades and Post-Election Audits

As of 2018, Pennsylvania was one of the small minority of states still primarily voting on paperless Direct Recording Electronic (DRE) voting systems. In April 2018, DOS directed all 67 counties to purchase new voting systems that meet current security and accessibility standards, and which include a voter-verifiable paper record with plain text language that voters can verify before casting their ballot and that local officials can use in recounts and post-election audits. These new systems must be in use no later than by the primary of 2020, and preferably by the November 2019 election.

In order to bolster our voting system security even further, in 2018 DOS created new security standards by which to evaluate the new voting systems applying for certification in PA. PA law requires both federal and state certification, and because the federal EAC had not updated its standards in some time and did not have a quorum to do so at the time, we decided to update our state security standards, and additionally assess the accessibility of the systems. The new voting system standards incorporated tests to ensure confidentiality, vote anonymity, integrity, security, auditability, and usability of the voting systems. All new certified systems in Pennsylvania have passed the following tests:

- Penetration testing that evaluates the security of the voting system by trying to exploit potential vulnerabilities.
- Access control testing to confirm that the voting system can detect and prevent unauthorized access to the system and election data.
- Evaluation of voting system audit logging capabilities to confirm that the system logs will allow auditing, as well as investigation of any apparent fraudulent or malicious activity.
- Tests that ensure every physical access point is well secured and system software and firmware is protected from tampering.

To evaluate accessibility of voting systems for voters with disabilities, we utilized expert review by usability and accessibility examiners as well as feedback from voters with disabilities and poll workers.

DOS has certified seven new voting systems that meet these standards, and we are very pleased with the remarkable progress made by the counties. The county election directors and commissioners have been incredibly dedicated to acquiring voting systems that best meet their voters' needs and provide the most secure, auditable, and accessible voting systems to all Pennsylvanians. Already, 75 percent of counties have officially voted to select new systems, and 46 out of 67 counties are utilizing their new systems with verifiable paper records in November 2019. The remaining counties are still hard at work planning and evaluating their voting system choices, reviewing vendor quotes and prices, holding new voting system demonstrations for the public, consulting with voters and poll workers and exploring funding and financing options.

Cost, of course, remains a major concern for counties. Since the beginning of this initiative, we have been committed to this enterprise being a cost-share of federal, state, and local dollars. Toward this end, we designated 100% of the federal funds appropriated in 2018 for election security proportionately to the counties for replacement of their voting systems by 2020, totaling $14.15 million in PA (including a 5% state match). Though a welcome down payment and approximately 10-12% of the total costs of the new systems, $14.15 million is not nearly enough, and we are pursuing additional state and federal funding.

We have also formed a statewide post-election audit working group, which includes election officials from six counties of different sizes and demographics across the state, as well as expert advisors on audits and elections. This working group is studying audit models such as risk-limiting audits and is developing best practice recommendations for post-election audits that will review the plain text on the paper records and the tabulated votes to confirm to a reasonable degree of statistical certainty the accuracy of the outcome of the election.

The dedication and thorough examination by the members of this workgroup to developing effective models has been inspirational and should be a model for other states looking to explore these practices. In addition, two of our counties on opposite sides of the state, Philadelphia and Mercer county, have volunteered to pilot advanced post-election audits this November 2019,

which will offer confidence to the voters as well as the opportunity to establish and test real-time best practices. Additional Pennsylvania counties will also be piloting audits over the next several years, and we expect all counties to employ enhanced audits by the 2022 general election.

Looking Forward

Looking forward, we continue to build. The above initiatives have taken and will continue to take significant resources to advance. In addition to advancing and strengthening all of the above, our highest priority goals and need for additional resources include: replacing our statewide voter registration system (SURE); ensuring all counties have advanced intrusion detection systems and practices, ongoing and evolving comprehensive cyber hygiene assessments, COOP and security training, and vulnerability assessments; and implementing new voting systems, strengthened pre-election testing, and enhanced post-election audits statewide.

CONCLUSION

On Election Day 2018, we saw what happens when all of the collaboration and hard work comes to fruition, and the powerful benefits of the intersection of all of the above in action. We were connected throughout the day to the counties, state agencies, other states, and the federal government through shared dashboards and frequent communications. For example, if another state was seeing attempted attacks coming from particular IP addresses, they were able to share with other states, allowing us to block those IP addresses at the state level, and then Pennsylvania would share those IP addresses with all 67 counties to enable them to block those IP addresses as well. We had conference calls throughout the day with our interagency group members and counties, sharing what we were hearing and seeing, any concerns, and any support or resolutions we could provide from our different sectors. This collaboration and communication allowed us to be proactive in our defenses, rather than just reactive as might have occurred in the past.

The right to vote is a fundamental right, and every voter must be provided equal access to the polls and deep-seated confidence in the security and accuracy of their vote. We cannot allow circumstances to develop whereby voters in under-resourced counties have less security or less accessibility in their vote. Pennsylvania — where both the Declaration of Independence and the U.S. Constitution were adopted — takes its legacy as the birthplace of American democracy very seriously, and we know that the foundation of that democracy rests on the security, auditability, accessibility and integrity of our elections. We urge you please to invest additional funds to ensure this for ourselves and for generations to come. Our democracy - and bolstering voters' confidence in their ability to participate fully in that democracy - is worth every dollar.

Thank you for the opportunity to testify on this important issue, and I am happy to answer any questions you may have.

Chairman NADLER. Thank you.
Mr. Burt?

TESTIMONY OF TOM BURT

Mr. BURT. Chairman Nadler, Ranking Member Collins, and Members of the committee, thank you for the opportunity to testify today on the important topic of how emerging technology can contribute to the security of our elections.

My name is Tom Burt. I'm the corporate vice President for customer security and trust at Microsoft. My team includes our Defending Democracy Program, which works to protect democratic elections from cyber-attack around the world.

We know that skilled and well-financed adversaries have and certainly will continue to attack elections in the U.S. and in other countries, all in the pursuit of their goal of undermining citizen confidence in democracy.

Defending democracy and our elections are important to Microsoft, so we spent the last year working on what we, as a technology provider, can contribute to this effort. I'm pleased to inform the Committee that this week we released a free, open-source software development kit called ElectionGuard.

Simply put, ElectionGuard technology can enable the most secure and trustworthy elections in the history of the United States. How does it do this? When a vote is cast, it is immediately encrypted so that it can't be seen or changed. The voter then receives a tracking number, and when the election is complete, the voter can go online and check to see, for the first time in history, that their vote was in fact counted and unchanged.

ElectionGuard, more than that, also enables anyone—voting officials, the media, third-party watchdog organizations—to build a verifier application that will let them confirm that the tally is correct and unchanged. All of this can be done without ever decrypting individual votes through the use of homomorphic encryption, a well-established technology that can count votes without ever decrypting the underlying data.

ElectionGuard is designed to work with many of the voting systems in use today, including electronic ballot-marking devices or hand-marked paper ballots read by optical scanners, and we have on our roadmap making it work with other forms of elections.

We have made this technology free and open to everyone. Microsoft is not making any revenue from ElectionGuard. We've been working closely with all the major U.S. election vendors, encouraging them to build systems with ElectionGuard, and we're excited to report that their response has been uniformly enthusiastic.

There is a significant impediment to the rapid adoption of this and other new voting technologies: The complex and outdated Federal election machine certification process. This process is more than a decade old, and it's too slow and too burdensome to enable voting officials to respond as quickly as needed to our agile adversaries. Unfortunately, this means that new machines using ElectionGuard likely will not be certified in time for use in the 2020 national election.

This certification process also hinders basic security hygiene. Today, if a voting machine is updated with a minor security patch

from a trusted vendor, it will have to go through a full recertification process. This creates a significant disincentive for election officials and vendors to deploy security patches, leaving our elections vulnerable.

We're pleased that the Election Assistance Commission is in the process right now of revising these certification rules, and we would ask all of you to encourage the Commission to adopt soon new rules that enable rapid and agile deployment of new security technology and basic security hygiene.

While we and others in the private sector can contribute technological advances to secure the vote, there is, of course, an important role for Congress. We agree with Ms. Plunkett's written testimony regarding the urgent need for long-term, sustainable funding. This is critically needed to enable election officials to plan ahead, to purchase new equipment rather than letting outdated systems remain active, and to invest in cybersecurity training and staffing that we expect of all critical infrastructure providers.

We live in a world with agile enemies who are persistent in their efforts to interfere in our democratic process. Our citizens deserve to be able to cast their vote with confidence that it will be counted without manipulation.

We believe ElectionGuard is breakthrough technology that can help achieve this goal. We remain committed to working with government, civil society, and the technology sector to take even more steps to ensure that every vote is counted and every voter has confidence in our free and fair elections. The stewardship of our democracy requires nothing less.

Thank you, and I look forward to your questions.

[The statement of Mr. Burt follows:]

Written Testimony of
Tom Burt

Corporate Vice President
Customer Security & Trust
Microsoft Corporation

to the House Judiciary Committee
to discuss emerging technologies and the security of US elections
September 27th, 2019

Chairman Nadler, Ranking Member Collins, Members of the Committee, thank you for the opportunity to testify today on the important topic of how emerging technology can contribute to the security of our elections.

My name is Tom Burt and I am the Corporate Vice President of Customer Security and Trust (CST) at Microsoft, a cross-disciplinary team made up of engineers, lawyers, policy advocates, business professionals, data analysts, and cybercrime investigators who are collectively responsible for ensuring customer trust in Microsoft's products and online services[1]. We focus on advocating for and contributing to the stability and security of democratic institutions globally. Specifically, last year we created the Defending Democracy Program. This team works with a variety of governmental and non-governmental stakeholders in democratic countries globally to achieve the following goals:

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

[1] 60 Minutes, April 21, 2019: https://www.cbsnews.com/video/a-marriage-made-in-hell-superbugs-easter-island/

THREATS AGAINST DEMOCRATIC INSTITUTIONS

Microsoft's work to preserve and protect our electoral processes and institutions builds upon the company's experience in assessing and tracking cybersecurity threats. The Microsoft Threat Intelligence Center (MSTIC) has focused on tracking nation-state actors for more than a decade. We provide notification to customers, including government customers, when an online service account has been targeted or compromised by a nation-state actor that is tracked by the MSTIC team.

In the past year, Microsoft notified nearly 10,000 customers[2] that they've been targeted or compromised by nation-state attacks. About 84% of these attacks targeted our enterprise customers, and about 16% targeted consumer personal email accounts. While many of these attacks are unrelated to the democratic process, this data demonstrates the significant extent to which nation-states continue to rely on cyberattacks as a tool to gain intelligence, influence geopolitics or achieve other objectives.

The majority of nation-state activity in this period originated from actors in three countries – Iran, North Korea and Russia. We have seen extensive activity from the actors we call Holmium, Phosphorus, and Mercury operating from Iran, Thallium operating from North Korea, and two actors operating from Russia we call Yttrium and Strontium. This data has been compiled by MSTIC which works every day to track these global threats. We build this intelligence into our security products to protect customers and use it in support of our efforts to disrupt threat actor activities through direct legal action or in collaboration with law enforcement. But let's be clear – cyberattacks continue to be a significant weapon wielded in cyberspace. In some instances, those attacks appear to be related to ongoing efforts to attack the democratic process.

Last August Microsoft instituted enhanced cybersecurity services for campaign users of Office 365 and free email services[3]. The program is called AccountGuard, and since its launch in 2018 we have uncovered attacks specifically targeting organizations that are fundamental to democracy. We have steadily expanded AccountGuard to political campaigns, parties, think tanks, and democracy-focused

[2] "New cyberthreats require new ways to protect democracy", July 17, 2019: https://blogs.microsoft.com/on-the-issues/2019/07/17/new-cyberthreats-require-new-ways-to-protect-democracy/
[3] "We are taking new steps against broadening threats to democracy", Aug 20, 2018: https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/

nongovernmental organizations (NGOs), in 26 countries across four continents. While this service is relatively new, we've already made 838 notifications of nation-state attacks targeting organizations participating in AccountGuard. This data shows that democracy-focused organizations in the United States should be particularly concerned as 95% of these attacks have targeted U.S.-based organizations. By nature, these organizations are critical to society but have fewer resources to protect against cyberattacks than large enterprises.

Many of the democracy-focused attacks we've seen recently target NGOs and think tanks and reflect a pattern that we also observed in the early stages of some previous elections. In this pattern, a spike in attacks on NGOs and think tanks that work closely with candidates and political parties, or work on issues central to their campaigns, serve as a precursor to direct attacks on campaigns and election systems themselves. Similar attacks occurred in the U.S. presidential election in 2016 and in the last French presidential election. In 2018 we announced attacks targeting, among others, leading U.S. senatorial candidates and think tanks associated with key issues at the time[4]. Earlier this year we saw attacks targeting democracy-focused NGOs in Europe close to European elections[5]. As we head into the 2020 elections, given both the broad reliance on cyberattacks by nation-states and the use of cyberattacks to specifically target democratic processes, we anticipate that we will see attacks targeting U.S. election systems, political campaigns or NGOs that work closely with campaigns.

Our adversaries have a stated goal of seeking to diminish the confidence of our citizens in the processes that are at the very core of our democracy. We should anticipate that we will see more attacks on our election processes in 2020 in furtherance of this goal.

MULTI-STAKEHOLDER RESPONSE

Combatting these attacks will require a joint effort from private sector actors such as Microsoft, as well as state, local and federal governments, civil society, academia, and voters themselves.

---

[4] "Microsoft Says It Stopped Cyberattacks on Three 2018 Congressional Candidates", Time, July 19,2018: https://time.com/5343585/microsoft-candidate-cyberattacks/

[5] "New steps to protect Europe from continued cyber threats", Feb. 20, 2019 https://blogs.microsoft.com/eupolicy/2019/02/20/accountguard-expands-to-europe/

Cyber-attacks, especially ransomware attacks, are increasingly targeting state and local authorities, including for example, Atlanta (GA), Baltimore (MD), Cleveland (OH), Greenville (NC), Imperial County (CA), Stuart (FL), Augusta (ME), Lynn (MA), Cartersville (GA). Most recently there was an attack on over twenty government entities in Texas. Overall, we can reasonably expect that the situation will only get worse. Importantly, these and other attacks are increasingly leveraging sophisticated tools that are developed by governments, creating a dangerous ecosystem of cyber-weapons and requiring adoption of international norms for responsible behavior online. Through our Digital Diplomacy team in CST, Microsoft works to advance support for the adoption and observance of such norms.

Microsoft supports the multi-stakeholder approach taken by the Paris Call for Trust and Security in Cyber Space[6]. It reaffirms a number of norms and principles established in other forums, including at the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN-GGE), and at the G7 and G20, respectively. Importantly, the Paris Call includes a comparatively new principle to protect electoral processes from foreign interference - *Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities.*

However, what truly distinguishes the Paris Call is that it recognizes that a multi-stakeholder approach is essential to achieve success. The Call has so far been signed by 67 nations, 139 civil society organizations and 358 industry members all agreeing to nine core principles to govern conduct in cyberspace. Microsoft was one of the private sector signatories and we will continue to advocate that all governments agree to observe the nine principles of the Call.

SECURING EXISTING ELECTION SYSTEMS

As the Senate Intelligence report on Russian interference in the 2016 U.S. elections[7] recently confirmed, at least 21 states had their election systems targeted by Russian actors, likely more. While the report states there was no

[6]Paris Call for Trust & Security in Cyber Space: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

[7] Report of the Selection Committee on Intelligence United States Senate: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf

evidence found to indicate vote tallies or voter registration systems were deleted or modified, the adversary succeeded at what was likely their primary goal – undermining U.S. voter's trust and confidence in our electoral system.

The undermining of such a vital democratic institution should cause us all alarm. At Microsoft, our Defending Democracy team began to review election infrastructure in the U.S. to identify areas where we could make a unique contribution to the security of our elections and restore voter confidence.

One surprising thing we identified was the active use of Windows 7 on several certified voting systems. For context, Windows 7 was launched by the company in 2009, and therefore represents decade-old security engineering. At that time we committed to supporting Windows 7 for ten years, and so in January of 2020 Windows 7 will reach its end of life and no longer be a supported operating system.

As we head into the 2020 elections though, knowing that many certified election systems are running Windows 7 without access to security patches does not sit well with us. With that in mind, last week we decided to offer free Windows 7 Extended Security Updates (ESUs) to federally certified election systems in the US through the end of 2020.[8] We have worked with the major election vendors to ensure they have access to these ESUs and are able to deploy them to customers as needed. We also are working with vendors who do not have a Windows 10 offering currently in the market to provide technical guidance and support as they make that transition.

STANDARDS AND CERTIFICATION

Providing free security updates does not completely solve the problem, however. A critical challenge to advancing the technical security of our vote is the complex and outdated federal election machine certification process. The current standards by which election machines are being certified today are even older than Windows 7!

The certification process has significant limitations that can stifle the introduction of advanced technology into this market, but also hinders basic security hygiene.

[8] "Extending free Windows 7 security updates to voting systems", Sep 20, 2019: https://blogs.microsoft.com/on-the-issues/2019/09/20/extending-free-windows-7-security-updates-to-voting-systems/

In the current system, if a certified device were to accept a minor security patch, it would be subjected to the same complete re-certification process that would be necessary for a major software update. This creates a perverse disincentive for election officials and vendors to deploy security patches to their machines, leaving our elections vulnerable via a self-inflicted wound.

In 2002, the Help America Voting Act (HAVA) created the Election Assistance Commission (EAC) to set voting system standards, provide for the testing and certification of those voting systems, establish guidelines against which those systems are certified, and accredit independent non-federal laboratories that certify voting systems[9]. The EAC certifies voting systems against the Voluntary Voting System Guidelines (VVSG). In 2005, the EAC updated the 2002 Voting System Standards (VSS) in collaboration with the Technical Guidelines Development Committee (TGDC) and the National Institute for Standards and Technology (NIST). These updated 2005 Voluntary Voting System Guidelines (VVSG 1.0) for the first time added security requirements to the certification criteria. Of the 57 currently certified voting systems, 52 are certified against the VVSG 1.0 and 5 against the 2002 standard that did not include security requirements. The EAC has further modified the VVSG 1.0 and created the VVSG 1.1 to "enhance the testability and clarity of several of the requirements contained in version 1.0." No voting systems have ever been certified to VVSG 1.1; most systems in use were thus certified to a 2005 standard. In the world of cybersecurity, this is ancient times.

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

[9] 52 U.S.C. § 20971.

maintaining certification by using a system with a known vulnerability. With today's threats, from agile and well-resourced adversaries attacking our election systems, this impediment to the rapid deployment of security updates is simply untenable and must be promptly rectified.

The EAC is now in the process of developing VVSG version 2 and has published the Technical Guidelines Development Committee recommendations – the VVSG 2.0 Principles and Guidelines document[10] – for comment. Notably, the Principles and Guidelines allows for software updates, though the details of how security updates will be applied to systems without triggering a comprehensive certification process is still unclear.

Microsoft has submitted comments on the VVSG 2.0 Principles and Guidelines. Those comments describe its strong support for the guidelines as an important step towards improving election technology security in the United States. Recognizing that diversity in organization, systems, networks, and assets of the elections infrastructure expands the attack surface and increases the risk of a cyber-attack altering elections results, Microsoft's comments specifically emphasize its support for the VVSG 2.0 guidelines on auditability. Microsoft strongly encourages the rapid adoption of VVSG 2.0 guidelines with provisions that support a much more agile and rapid process for the adoption and deployment of secure election technology.

INNOVATIVE ELECTION TECHNOLOGY - ELECTIONGUARD

Outdated standards not only impact the security of our existing systems, they serve as a hurdle for the introduction of new and innovative technology. We know this firsthand, as just this week we released a free, open-source software development kit (SDK) called ElectionGuard that will enable **end-to-end (E2E) verifiable (E2E)** elections.[11] **Simply put, ElectionGuard technology will enable the most secure and trustworthy elections in the history of the United States**.

In an end-to-end-verifiable election, any alteration or incorrect counting of votes can be detected by candidates, political parties, news outlets or interest groups; and this capability extends not only to external threats but even to potential

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

[11] "ElectionGuard available today to enable secure, verifiable voting", Sept. 24, 2019: https://blogs.microsoft.com/on-the-issues/2019/09/24/electionguard-available-today-to-enable-secure-verifiable-voting/

internal threats by faulty or malicious equipment or by overworked or even dishonest election officials. Even more importantly, individual voters will be able to verify that their votes were recorded and counted properly.

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

ElectionGuard builds on Microsoft Research Senior Principal Cryptographer Josh Benaloh's foundational work on E2E- verifiability[12] accomplished through the use of homomorphic encryption. The ElectionGuard open-source SDK is available on GitHub[13] for anyone to review, though we have been working closely with all the major US election vendors, encouraging them to incorporate the code directly into their systems.

ElectionGuard is intended to augment – rather than replace – existing voting systems. It can be used in conjunction with a variety of voting scenarios including electronic ballot marking devices and hand-marked paper ballots read by precinct-based optical scanners. The voting processes will be almost identical to the processes that voters use and are familiar with today - with one exception.: Voters will receive and be able to leave their polling locations with printed tracking codes and instructions for how they can, if they choose, confirm their votes were properly counted when the election closes[14].

Ballot privacy is critical in elections. Elections have the unusual, perhaps even unique, requirement of not allowing participants to reveal their data – even if

---

[12] Written Testimony of Josh Benaloh to Subcommittee on Investigations & Oversight and the and the Subcommittee on Research & Technology: https://science.house.gov/imo/media/doc/Benaloh%20Testimony.pdf

[13] GitHub is the largest developer community in the world, and the home of 80% of all active open source projects. And it's more than just open source - more than 2 million organizations that use GitHub for their software projects, including the vast majority of technology startups and 50% of the Fortune 100

[14] We acknowledge this solution depends on the voter having access to a smart phone or to broadband connectivity. Microsoft notes that broadband connectivity is also an urgent national problem that we are committed to helping solve. We've contributed to this effort through our Microsoft Airband Initiative, a five-year commitment to bring broadband access to 3 million unserved Americans living in rural communities by July 2022. Microsoft is partnering with a number of local providers across the US to offer new broadband services where there is no option or affordable alternative.

they choose to do so. A voter who can reveal a vote to someone else can sell that vote or be coerced into voting according to the wishes of another. With ElectionGuard voters can verify the accurate recording of their votes but cannot use their tracking codes to reveal their votes, and their privacy is thus protected.

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

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

DEMONSTRATION MACHINE AND ACCESSIBLE VOTING

To showcase the ElectionGuard technology, we have constructed reference implementation devices that demonstrate how it could be incorporated into low cost, secure and accessible voting machines. This demo system is not intended for sale – rather it exists to showcase the ElectionGuard code while highlighting other features that may be considered for new voting systems. At Microsoft our products are built to empower everyone, everywhere. [15] That principle applies to voting as well where accessibility is a paramount consideration for all voting officials. We therefore designed ElectionGuard to support a range of accessibility features including the Xbox adaptive controller for certain physical disabilities and

[15] Microsoft Accessibility: https://www.microsoft.com/en-us/accessibility

interfaces for other accessibility systems. We have several of these demo systems in our Redmond and DC offices and invite Members of the Committee to a demonstration of how emerging technology can be used to improve the security and accessibility of our elections.

Figure 1 Microsoft employees testing an ElectionGuard demonstration system at the Aspen Security Forum

PAPER BALLOTS

As noted above, ElectionGuard is designed to support a wide range of voting systems and will continue to be enhanced to support others. In our reference implementation we demonstrate a system with a highly efficient, convenient and accessible ballot marking device which supports printed ballots that can be deposited and retained by voting officials as either the primary artifact or as a back-up. The recent debate about the security of voting devices has resulted in some calling for a return to manually marked paper ballots exclusively. While paper can be a helpful tool, it is not a goal in and of itself. The goals of ElectionGuard technology are to ensure security, trustworthiness, accessibility and efficiency – goals that can be achieved whether paper is used as primary artifact or backup, but which cannot be fully realized without ElectionGuard.

PROTECTING POLITICAL ACTORS

Attempts to interfere with the electoral process extends to the political campaign environment as well, which has been very much in focus at the Federal Election Commission (FEC) over the past year. Though much attention has been given to the Russian "Internet Research Agency's" attempts to sow discord through online propaganda targeted at American voters, the hacking of the online accounts of political operatives and party committees was also a key attack mounted by Russia and must not be overlooked.[16]

With more than 60 million users of its paid Office365 (O365) cloud-based productivity software and free Outlook.com and Hotmail.com web-based e-mail services, Microsoft found itself in a unique position to protect election-sensitive users of its products against such hacking. To that end, Microsoft requested and received an advisory opinion from the FEC confirming that Microsoft may offer a package of free enhanced online account security protections at no additional charge on a nonpartisan basis to its election-sensitive customers. The FEC issued an Advisory Opinion concluding that the provision of AccountGuard is permissible and is not a prohibited in-kind contribution under campaign finance law.[17]

Until this advisory opinion, the FEC had not robustly addressed the provision of cybersecurity services to political campaigns and national committees. In response, this advisory opinion sparked a series of similar requests for approval[18] from cybersecurity firms to provide cybersecurity services to members of Congress, political campaigns, and national committees.

Political campaigns are fast-moving environments that face significant security threats from nation-state actors and criminal scammers – much like large enterprises. However, unlike enterprises, political campaigns often must ramp up and down quickly, vary in their ability to hire dedicated IT staff, and have

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

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

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

unpredictable budgets. In some cases, they rely on scrappy "accidental administrators" who help with IT on the side; in other cases, they have experienced IT consultants but need to focus their budgets on getting out their candidates' message.

For these reasons, Microsoft recently announced the availability of Microsoft 365 for Campaigns.[19] The Microsoft 365 for Campaigns sign-up process allows for streamlined enrollment into Microsoft's AccountGuard service and is available at a price of just $5 per user per month – the same price as offered to nonprofits and nongovernmental organizations. Microsoft 365 for Campaigns, brings the high-end security capabilities of the Microsoft 365 Business offering – with specialized "wizards" to make it easy to deploy – to political campaigns at this reduced rate on a nonpartisan basis.

EMERGING THREATS

A few weeks ago CISA Director Chris Krebs drew attention to the threat of ransomware attacks against our local governments and the impact that could have on our elections if executed against voter registration systems close to, or on, election day.[20] We agree this is a risk that deserves attention from all election security stakeholders. Voter registration databases (some of the same systems targeted in 2016), are vulnerable because they are some of the only election sensitive systems that are regularly connected to the internet. We have advised Director Krebs that we stand ready to participate with CISA and others in the tech community to seek solutions, including providing all election officials with simple step-by-step recommendations on important security hygiene such as two-factor authentication for all relevant accounts, how to secure registration and other data systems, establish secure back-ups, and engage in exercises to ensure rapid restoration of data in the event of an attack.

An additional emerging threat is the increased potential for bad actors to use artificial intelligence to create malicious synthetic media, better known as "Deepfakes". Advances in synthetic media have created clear benefits; for example, synthetic voice can be a powerful accessibility technology, and synthetic

[19]"Protecting political campaigns from hacking", May 6, 2019: https://blogs.microsoft.com/on-the-issues/2019/05/06/protecting-political-campaigns-from-hacking/

[20]"CISA Director's Outlook on Ransomware", Aug 23, 2019: https://www.politico.com/newsletters/morning-cybersecurity/2019/08/23/cisa-directors-outlook-on-ransomware-5g-more-727286

video can be used in film production, criminal forensics, and artistic expression. However, as access to synthetic media technology increases, so too does the risk of exploitation. Deepfakes can be used to damage reputations, fabricate evidence, and undermine trust in our democratic institutions. To help guard against this challenge, Microsoft has established clear principles that govern its use and deployment of synthetic media and other artificial intelligence, including fairness, inclusiveness, reliability & safety, transparency, privacy & security, and accountability. Furthermore, Microsoft has engaged with partners in academia, civil society, and industry through forums like the Partnership on AI, where we can work together to advance best practices for the ethical use of AI and we and others are working on technical solutions to abuse of synthetic media systems.

CONGRESSIONAL ACTION

We applaud the Senate for its recent bi-partisan agreement to release additional funding to the states. This is an essential step in the right direction to equip local officials and to protect our election systems. But there is still more to be done. In our discussions with voting officials around the country we have learned that consistent and reliable funding over time will best enable election officials to plan ahead, purchase new equipment rather than letting outdated systems remain active, and invest in the kind of cybersecurity training and staffing that we expect of all critical infrastructure providers. Our adversaries are relentless and well resourced. To ensure we can maintain defenses, our state and local voting officials need a durable source of federal financial support so that the most secure technology can be deployed rapidly to ensure our vote is protected. The stewardship of our democracy demands nothing less.

In addition to funding, we need certification standards that are responsive to current technology and threats. Standards should incentivize security patching and updates, not create red tape that stands in the way of cyber best practices. While there are constructive conversations ongoing at the EAC, the pace of adoption and execution is slow, and the path to minimal security updates is still unclear. We hope Congress will encourage their colleagues at the EAC to pursue a speedy path to new standards, and in that process select a format that does not allow outdated standards to burden adoption of the most secure technology in the future.

Finally, Congress should encourage a multi-stakeholder and global commitment to pursue practical projects that are essential to protecting our online world. We must particularly strengthen our collective capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities.

CONCLUSION

We live in a world with agile enemies who are persistent in their efforts to interfere in our democratic process. Voters are looking to us – private industry and federal and local governments – to be leaders. Our citizens deserve to be able to cast their vote with confidence that it will be counted without manipulation. We at Microsoft are committed to doing our part to ensure that every vote is counted and that every voter has confidence in our free, fair and democratic elections.

Chairman NADLER. Thank you.

I thank all the witnesses for their testimony.

We'll now proceed under the 5-minute Rule with questions. I will begin by recognizing myself for 5 minutes.

I'd like to focus initially on one component of our election systems that I find particularly concerning: voter registration databases.

The Mueller report concluded that in approximately June 2016 the Russian intelligence organization GRU "compromised the computer network of the Illinois State Board of Elections" and "gained access to a database containing information on millions of registered Illinois voters," unquote.

Ms. Plunkett, in this case, the Russian hackers successfully breached the databases, but they failed to alter or to delete voting records. My question to you is, if Russian hackers had changed voting records, including deleting voters from the databases, can you describe the specific possible impacts it could've had on the election?

Ms. PLUNKETT. If they—

Chairman NADLER. If they had altered the databases.

Ms. PLUNKETT. Well, it would've been devastating had they altered the databases. "Altering" in this case could've been changing records; it could've been deleting records, which would have made it, in some cases, impossible for voters to vote, to register to vote. Voters could've been turned away. It could've inserted voters erroneously into the database that could've provided an opportunity for those who shouldn't be voting to vote. So, it would have been devastating had that happened.

Chairman NADLER. So, thousands or tens of thousands of voters might have turned up at the polls and been turned away because—

Ms. PLUNKETT. That's correct.

Chairman NADLER. —there was no record of their registration?

Ms. PLUNKETT. That's correct.

Chairman NADLER. Thousands of nonexistent voters might have voted?

Ms. PLUNKETT. That's correct.

Chairman NADLER. Thank you.

Ms. Plunkett, the House-passed appropriations bill contains $600 million in funding for States. It also includes accountability measures and requires that funding cannot be used to purchase nonqualified voting machines. The Senate's version has only $250 million, with no accountability restrictions.

Your written testimony emphasizes the need to replace paperless machines and implement robust post-election audits using paper ballots.

Now, we saw in 2000 how one county's failure to properly maintain its chads or non-chads held up the entire country. One county's dereliction could again conceivably hold up the entire country's election, national election.

Now, I understand why some States or counties might not want to spend the money necessary to update their election machinery so they can't be hacked, but I was astounded to read recently, a couple days ago in fact, that States are still buying, spending large amounts of money, on voting machines that are electronic, that do

not have paper trails, that are unauditable and vulnerable to hacking.

So, my question is, aside from the obvious necessity of appropriating money to update our election machinery so that we have hack-proof machines that cannot be tampered with from the outside and that leave auditable trails, which means paper trails, do you think that the Federal Government should mandate this? Because, after all, the Federal elections are premised on accurate counts in every State and county. Should we mandate as well as providing the funds for modern election technology so that we can be sure that no foreign actor is in fact hacking it, in fact, phonying up our vote, and perhaps even doing so and leaving no trail so that you knew it later?

Ms. PLUNKETT. So, woe is me to make a comment about Federal and State roles and responsibilities, but here's what I'd say, sir: It is incumbent upon every State to institute the appropriate security measures and make sure that their technology is their most robust available in order to protect the democracy and their election and votes.

I believe that there's a role for the Federal Government in this space that starts with requiring that vendors follow certain security standards in the production and delivery and maintenance of the equipment that these States are using. That would thereby standardize, at least, the security of those systems, everything from auditing and database management to, on the back end, should something happen to the systems, being able to report on that.

Chairman NADLER. So, obviously, if the Federal Government mandated that only proper machines could be made, then new purchases would only be of proper machines.

In the 5 seconds I've got left, do any of the other witnesses want to comment on whether they think it necessary for the Federal Government to mandate that existing machines be replaced in time for the next election so that we can guarantee an election un-dictated from Moscow or someplace else?

Mr. BURT. We think, as the Election Assistance Commission is revising its standards for certification, there's an opportunity there to inject standards for the security of devices to be certified. I would caution, though, that we must be careful not to specify specific technological solutions—

Chairman NADLER. Right.

Mr. BURT. —because our enemies move very quickly. We need to be agile in response.

To have basic security guidelines that are part of that certification process would be an advance in the current State and would help us secure our elections.

Chairman NADLER. Thank you.

Ms. Boockvar, quickly, because my time has expired.

Ms. BOOCKVAR. Chairman, I just want to say that I think you've mentioned a lot of the areas that we need to invest. You talked about voter registration systems. I think you talked about sensors, intrusion-detection sensors, and all kinds of other things.

So, what I'd like to see is that we define a continuum, a number of different things that are critical priorities, but allow the States,

who know best what's the most critical need in their State, to decide what the best use of those funds are.

Chairman NADLER. Thank you very much.

My time has expired.

The gentleman from Colorado.

Mr. BUCK. Thank you, Mr. Chairman.

Mr. Burt, I'm interested in the ElectionGuard technology that you were talking about earlier. One of the interests I have is that the United States wasn't the only country that Russia targeted in the last decade. It's clear that Russia tried to impugn the integrity of the Brexit vote, the Scottish independence vote. They've been involved in Spain with the Catalonia independence movement.

Will Microsoft make ElectionGuard available to our allies, foreign countries, or something similar, so that we can try to make sure that democracies across the world have elections that are considered by their people to have integrity?

Mr. BURT. Yes, that's absolutely our plan, Congressman. As you may know, our AccountGuard service, which we offer for free to help protect campaigns against being hacked, we've extended that now to 26 countries around the world, and we intend to do the same with ElectionGuard technology as well.

It is a free, open-source project, so any vendor in any country is free to take that technology and build it into election systems. We work to expand our protections to all democracies committed to free and fair elections.

Mr. BUCK. Okay.

Mr. Burt, one of the things I'm interested in is exactly—you've used the word "agile" a number of times. I'm assuming that there is a distinction between hardware and software when you're talking about agility, and I'm wondering if you could just explain that.

When Chairman talks about, and rightfully, you know, updating systems, I think we're in large part talking about hardware. I want to make sure that we have hardware that's compatible with whatever the software is that we need to be agile with.

Mr. BURT. Yes, it's absolutely important that both hardware and software be the most secure, current engineering. There's work to do, frankly, on both sides of that. Most importantly, for most of these systems, it's the ability to update software.

As I mentioned in my written testimony, we just announced recently that we are going to provide free security updates to Windows 7 election voting devices, because we discovered that there are many of those devices still in operation around the country even though that's decades-old technology. It reaches its end of life this January for most customers, but because of the importance of securing our vote, we are providing for free those security updates through the end of 2020.

The challenge, though, is, as I mentioned earlier, with current regulations, it's actually very difficult and burdensome for local officials to even apply security patches to their devices. So, we need to work on both the software and hardware side of the equation to ensure that we can be agile in adopting the best technology to defend against these attacks.

Mr. BUCK. So, for old folks like me, we think that, if it's not on paper, it's not secure and it's not believable. I just want to open

this up for the young folks on the panel here, if you have an opinion on how we convince the American public. Because that's really the audience, in this case, is making sure the American public understands we're doing everything we can to make elections credible.

How do we convince the American public that something that we can't see, that exists out there somewhere, is just as good as a paper ballot and being able to see something on paper?

Mr. BURT. If I could start off, and at least I'll claim to be young at heart, Congressman. There are two really important things we can do to help establish that trust.

One which you've heard about from others, which we absolutely endorse at Microsoft, is the existence of a paper backup, at least, that can be used in risk-limiting audits. In fact, our ElectionGuard technology supports an advanced form of risk-limiting audits, which enables voting officials to audit the outcome after the vote and show that it wasn't tampered with.

So that's one important thing, is the application of audits and the maintenance of at least a paper backup so that you always have that as a resource to go to.

Again, if we can get to a world where the ElectionGuard technology is broadly adopted, that provides a whole new form of voter trust, because now voters will be able to, for the very first time, actually see that their vote got counted and wasn't changed. Today—I'm from Washington State—I have no idea whether the ballot I marked was ever actually counted or not. With this technology, voters will know, which should help establish voter trust.

Mr. BUCK. Thank you.

Mr. Chairman, I don't often do this, but I wanted to thank you for holding this hearing. I think this is beneficial. It has very little to do with partisanship. It's important for everybody on both sides of the aisle and all around the country, to make sure we have this integrity. So, thank you very much.

Chairman NADLER. Thank you.

The gentleman's time has expired.

The gentlelady from Texas.

Ms. JACKSON LEE. Thank you, Mr. Chairman. Let me add my appreciation for this very crucial hearing as well.

Thank you to all the witnesses.

Let me ask one question from each of you, with a "yes" or "no" answer. Do you think it is important for there to be governmental involvement in a regulatory structure, in review of the technologies, as we move toward the upcoming elections, as quickly as possible?

Ms. Plunkett?

Ms. PLUNKETT. Yes.

Ms. JACKSON LEE. Secretary Brockner?

Ms. BOOCKVAR. Boockvar. Yes.

Ms. JACKSON LEE. Mr. Burt?

Mr. BURT. Yes, I do.

Ms. JACKSON LEE. Let me ask, Ms. Plunkett, with respect to the 2016 election and the Russian GRU officers compromised a computer network of the Illinois State Board of Elections and gained access to a database containing information on millions of registered Illinois voters. The Russian GRU officers were able to steal

data of thousands of U.S. voters before Illinois was aware of the hack.

If Russia had succeeded in all these efforts, can you explain how attacking voter registration software in electronic polling stations can impact an election?

Ms. PLUNKETT. Certainly.

Since the foundation of the voter system begins with the registration databases, which validates that a voter is eligible to cast a vote, should that database be altered in any way, whether it be destroyed or deleted or additions made to it, it could jeopardize the ability of a legitimate citizen who has the right to vote from voting and would certainly alter the outcome of the election because it would prevent those who should be able to vote from casting their votes.

Ms. JACKSON LEE. In essence, it would undermine the very basis of our democracy.

Ms. PLUNKETT. That's correct.

Ms. JACKSON LEE. Mr. Burt, you've mentioned the ElectionGuard. We are all fascinated by that. It's outstanding technology.

In your marketing to the entire world, I'm not sure what kind of litmus test you're going to use to determine whether or not it is a democratic government. What is the potential of innocent democratic governments now giving technology of that level of sophistication to be utilized, then, to hack into the system? What are the protections and the firewalls on your system if, by chance, you sell it to an enemy, a foreign enemy?

Mr. BURT. Well, Congresswoman, we're actually being quite deliberate and careful about the countries to which we expand our services. Let me be clear about ElectionGuard: It's an open-source project that anyone can access. That actually leads to the security, because as people find any flaws or security flaws in that software, it can be updated.

What's important to understand is that this technology is not capable of being used as an offensive weapon. What it does is secure the vote. What it does is ensure that votes are encrypted and can't be changed or altered. It ensures that the vote can be verified and that the count can be properly verified by individual voters and by any third party.

So, to the extent that this technology is deployed even in countries that we would not consider an ally, it just means that their votes are going to be more trustworthy than they are today.

Ms. JACKSON LEE. So, it doesn't give them the ability to breach or to hack into the votes of another country?

Mr. BURT. That's correct.

Ms. JACKSON LEE. Let me ask Secretary Boockvar, what is the importance of having a variety of technologies that States can have access to, rather than the limited number of vendors that we already have, in terms of protecting the election process?

Ms. BOOCKVAR. So, I think one of the benefits that we have is—decentralized systems have their advantages and disadvantages, but having the variety of technology is definitely an advantage, because the likelihood of the ability to breach all the different technologies is certainly harder than if you had one uniform across the board. So, it's key to keep the diversity of our systems.

Ms. JACKSON LEE. You only have, I think someone mentioned three. So having us to be able to certify or legislation that deals with expanding that opportunity would also enhance the security and safety of elections.

Let me—you're all lawyers. In the past election, 2016, we've determined that there were a lot of foreign operatives. Do you think it's important to have legislation that indicates that if you, an elected official, or a candidate, are approached by a foreign adversary, that you need to report that immediately to an organization, agency, such as the FBI?

Ms. Plunkett? I'm just asking everybody across the board.

Ms. PLUNKETT. Yes, I do.

Ms. JACKSON LEE. Madam Secretary?

Ms. BOOCKVAR. Yes, I do as well, Congresswoman.

Ms. JACKSON LEE. Mr. Burt?

Mr. BURT. Certainly.

Ms. JACKSON LEE. I ask unanimous consent to place into the record H.R. 2353.

Chairman NADLER. Without objection.

[The information follows:]

MS. JACKSON LEE FOR THE OFFICIAL RECORD

I

116TH CONGRESS
1ST SESSION

H. R. 2353

To amend the Federal Election Campaign Act of 1971 to require candidates for election for public office to refuse offers of assistance from foreign powers and to report such offers to the Federal Bureau of Investigation, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

APRIL 25, 2019

Ms. JACKSON LEE (for herself and Mr. JOHNSON of Georgia) introduced the following bill; which was referred to the Committee on House Administration

---

A BILL

To amend the Federal Election Campaign Act of 1971 to require candidates for election for public office to refuse offers of assistance from foreign powers and to report such offers to the Federal Bureau of Investigation, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Duty to Refuse and Report Foreign Interference in American Elections Act of 2019".

SEC. 2. REQUIRING CANDIDATES TO REFUSE OFFERS OF ASSISTANCE FROM FOREIGN POWERS AND TO REPORT OFFERS TO FBI.

(a) REQUIREMENTS DESCRIBED.—Section 319 of the Federal Election Campaign Act of 1971 (52 U.S.C. 30121) is amended by adding at the end the following new subsection:

''(c) REQUIREMENTS FOR CANDIDATES RECEIVING OFFERS OF ASSISTANCE FROM FOREIGN POWERS.—

''(1) DUTY TO REFUSE ASSISTANCE AND REPORT OFFER TO FBI.—If a candidate or any individual affiliated with a campaign of a candidate knowingly receives an offer for assistance with the campaign from a source the candidate or individual knows is a foreign power or an agent of a foreign power, the candidate or individual shall—

''(A) refuse the offer for such assistance; and

''(B) notify the Federal Bureau of Investigation of the offer not later than 72 hours after receiving the offer.

''(2) CERTIFICATION REQUIREMENT FOR FEDERAL CANDIDATES.—Not later than 10 days after the expiration of each calendar quarter, each authorized committee of a candidate for election for Federal office shall file a report with the Commission

certifying that the candidate and the individuals affiliated with the candidate's campaign are in compliance with the requirements of paragraph (1).

"(3) PENALTY.—Whoever fails to comply with subsection (a) shall be fined not more than $250,000, or imprisoned not more than 5 years, or both.

"(4) DEFINITIONS.—In this section, the following definitions apply:

"(A) The term 'agent of a foreign power' and the term 'foreign power' each has the meaning given such term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

"(B) The term 'candidate' means an individual who seeks nomination for, or election to, any Federal, State, or local public office.

"(C) The term 'individual affiliated with a campaign' means, with respect to a candidate, an employee of any organization legally authorized under Federal, State, or local law to support the candidate's campaign for nomination for, or election to, any Federal, State, or local public office, as well as any independent contractor of such an organization and any indi-

vidual who performs services for the organization on an unpaid basis (including an intern or volunteer).''.

(b) EFFECTIVE DATE.—The amendment made by subsection (a) shall take effect 90 days after the date of the enactment of this Act.

○

Ms. JACKSON LEE. Can an effective deceptive campaign spoofing attack be deployed through user search engine requests?

I'll repeat it. Can an effective deceptive campaign spoofing attack be deployed through user search engine request?

Can you just answer the question, Mr. Burt?

Chairman NADLER. The time of the gentlelady has expired. The witnesses may answer the question.

Mr. BURT. Yes, that's possible, although a more fulsome answer would take a considerable period of time in terms of how that would work and how we can defend against it.

Ms. PLUNKETT. I agree, yes.

Ms. JACKSON LEE. All right. Thank you. I yield back.

Chairman NADLER. The gentlelady yields back.

The gentleman from Florida?

Mr. GAETZ. Thank you, Mr. Chairman.

I'd like to associate myself with the comments of the gentlelady from Texas and the gentleman from Colorado, that election security issues must be viewed as a bipartisan endeavor for us to be able to make progress and that all voters deserve to have confidence in that process.

I must say, it was a little disheartening that Chairman began the hearing by taking a bunch of partisan shots at the President. I don't understand how that is helpful to the work that we're doing here.

Really, thinking in terms of the value of elections most broadly, I fear that the greatest risk to our democracy may not be hacks or interference with the vote; it may be the efforts by radical Democrats to try to impeach a President who was duly elected. That seems to undo elections a lot more than hacking.

Alas, back to this important work of the committee. I wanted to thank Congresswoman Murphy as the lead but also our colleagues on the Judiciary Committee, Mr. Deutch and Ms. Mucarsel-Powell from Florida, for coauthoring H.R. 3529. This bipartisan legislation requires the head of the Department of Homeland Security to notify State and local election officials in the event of some intrusion or hack.

So my question is really to any of the Members of the panel to speak to the utility and importance of real-time coordination in the event of an intrusion and how you might see State and local officials working cooperatively and proactively with the Federal Government in such an endeavor.

Ms. BOOCKVAR. I'd love to take a crack at that. Thank you, Congressman.

It's critically important, that collaboration at the State, local, and Federal level. We saw it in Pennsylvania last year, in November of 2018's election. We were connected across the country to other States and to the Federal Government, getting real-time information about things that were being seen in other States.

We could not only take—so, for example, there were attempts to hack into—to send PDOS types of interruptions in other States. IP addresses were identified, passed along to other States. We then, in turn, were connected across the State to the 67 counties, could pass along those IP addresses, so they could block it proactively be-

fore having to have—it was literally in-action collaboration that protected our elections.

So that kind of thing, both before, during, and after, is critical to make sure that we have the most secure elections possible.

Mr. BURT. Congressman, if I may, in 2018, under the direction of Director Krebs from CISA, there was a war room established at the Federal level to which technology providers, State and local officials were all invited. We participated in that, and that was a good step forward.

What you suggest is absolutely critical. I agree that the more efficient we can have communication between all Federal agencies who are aware of attacks in real-time with State and local officials and, also, leading technology providers who stand ready to assist with this effort of protecting our elections, the better it can be.

So, we need to improve and expand on that rapid real-time sharing of threat information at the time of the election and before then.

Ms. PLUNKETT. I agree with both.

I'd just also add, it's critically important and a good role for the government to create the environment where information-sharing can happen without restrictions in a smooth and precise and expeditious manner, such that everyone who needs the information can get it and it's presented in a usable fashion.

I would not limit that to State, local, and Federal, as has already been stated. Vendors there are very good threat intelligence organizations that are doing a great job in uncovering good information that needs to be a part of this dialogue.

Mr. GAETZ. That is incredibly helpful advice, especially when I think about the experiences in Florida, where hackers masquerade as the vendors. So, they would seem to be an important part of that community. That's very helpful.

I would also observe that there seems to be some confusion in Florida as to the extent to which any hack could lead to voter manipulation in future elections, not based on changing the tallies of the votes but by potentially manipulating someone's name. I'm Matthew Louis Gaetz II, but if someone went and changed my name to just "Matt Gaetz" on the voter rolls, potentially I would have a hard time having my vote counted.

So, this may be a broader question than you're able to answer, but I am interested—and I think the Judiciary Committee could perhaps partner with others—on the utility of blockchain technology to enhance the security of elections. Because in an immutable, decentralized ledger, I would think that such a manipulation of the voter rolls, themselves, would be less likely.

I would seek any comment anyone would have.

I appreciate the chair's indulgence.

Ms. JACKSON LEE. [Presiding.] The witnesses may answer the question. The gentleman's time has expired.

Ms. PLUNKETT. I think there certainly the opportunity for blockchain to be relevant in this space. If we think now about the American public and their understanding of voting and voting systems, we are talking about paper ballots as a backup. Generally, people understand that.

Blockchain technology is very complicate and is untested. I know it's being tested in West Virginia, as I understand it. So, I think there's possibility, but it's not something that I think is ready for use for a general or primary election.

Ms. JACKSON LEE. The gentleman's time has expired.

The gentleman from Georgia is recognized for 5 minutes.

Mr. JOHNSON of Georgia. Thank you, Madam Chair.

Thank the witnesses for your appearance today and for your testimony.

Ms. Plunkett, the Center for American Progress recently reported that, quote, "voting on paper is the most hack-proof way of conducting elections." You agree with that, do you not?

Ms. PLUNKETT. Today, yes, I do.

Mr. JOHNSON of Georgia. What about you, Ms. Boockvar?

Ms. BOOCKVAR. Absolutely. At least with a paper record, I should say.

Mr. JOHNSON of Georgia. Uh-huh.

Mr. Burt?

Mr. BURT. Well, I would say that we actually believe that ElectionGuard provides an even more hack-proof way of voting. Paper as at least a backup or as primary—because the technology would support either—is important to maintaining the security of our elections.

Mr. JOHNSON of Georgia. Uh-huh.

So, when we talk about a paper ballot, we're talking about a hand-marked paper ballot.

Is that right, Ms. Plunkett?

Ms. PLUNKETT. It doesn't necessarily have to be hand-marked, but there should be a piece of paper involved that can be—

Mr. JOHNSON of Georgia. Well, now, if the paper involved is produced by a touchscreen voting machine and that piece of paper also has a barcode along with the races that the voter voted on, and this paper that the machine produces with the barcode is given to the voter, who can then check it, make sure that it reflects accurately what choices were made by that voter, and then that piece of paper is then scanned into a counting machine which counts not the actual choices made by the voter but the barcode on top, that's the kind of paper ballot that you're talking about?

Ms. PLUNKETT. I don't know about the barcode piece. I—

Ms. BOOCKVAR. So, I think I can answer that. So, for example, that's where audits come in, right? So, for example, we're developing a process in Pennsylvania where—

Mr. JOHNSON of Georgia. Well, I guess the question that I'm asking—if it's the barcode that is counted and not the box that is identified as the one that was checked by the voter, how does the voter know that the barcode which is counted actually reflects the choices that the voter made? Or does the voter just simply have to depend on the barcode to accurately reflect—how can we get around that if we're counting the barcode and not counting the hand-marked paper ballot?

Ms. BOOCKVAR. So, most systems, whether they're hand-marked paper ballot or ballot-marking devices, use some form of mark for the tabulation process, whether it's a barcode, a QR code, or timing

marks, which some of the hand-marked paper ballots use. So, there's basically triggers into the tabular, and then the audit—

Mr. JOHNSON of Georgia. Then you're able to actually count the hand-marked ballot by hand.

Ms. BOOCKVAR. Exactly. That's what the audit or a recount would do, would look at the plain text language on the—and it can compare to the tabulation numbers—

Mr. JOHNSON of Georgia. The tabulation of the machine.

Ms. BOOCKVAR.—yes, with the—

Mr. JOHNSON of Georgia. So, the hand-marked ballot is the way that it produces an auditable trail. The ballot that is counted by the barcode and is not hand-filled-out is just simply a further extension of the mechanics of the computerized voting?

Mr. BURT. If I may, Congressman. So, in the context we are talking about the barcode, that paper still shows the specific individual votes which the voter, in a well-run system, has had an opportunity to verify the checkmarks in the boxes. So, now you've got a—

Mr. JOHNSON of Georgia. Yeah, but those checkmarks are not the ones that are counted, though.

Mr. BURT. I understand. What I'm saying is—

Mr. JOHNSON of Georgia. It's the barcode.

Mr. BURT.—even if it's not hand-marked, if it's marked by the machine, but the voter has verified those boxes, now you have a paper ballot that's verified that can be used for counting.

Mr. JOHNSON of Georgia. How does the voter verify that the barcode or the counting mechanism accurately reflects the choices that the voter made?

Mr. BURT. Yeah, so that is part of the audit process that can be performed by looking at the tally against the audited subset of ballots that's selected for the audit, looking not at the barcode, in this case, but looking at the boxes that are checked. So, the audit system provides that.

Mr. JOHNSON of Georgia. Let me just say this, then. Isn't it clear that a hand-marked paper ballot that is then fed into a counting machine, which counts that tally, along with the other voters—and then, at the end of the voting process, if there is a recount, then you can actually count the paper ballot, the hand-marked paper ballot by hand and compare that to the tally that was produced by the counting machine, doesn't that provide the most effective way of auditing the results of an election?

Ms. JACKSON LEE. The gentleman's time has expired. The witness may answer the question.

Mr. BURT. I would say that it's not important whether the ballot was hand-marked or marked by a machine as long as the voter gets the opportunity to verify that what they see on the ballot is what they intended before they deposit it in the ballot box. Either way, whether it's my hand-marking or the machine that checks the box, you have a clear representation of the voter intent.

In fact, in the machine-checked box, sometimes that's clearer. As you know, with hand-marked ballots, there's often disputes about what a voter actually intended with the marking, depending on the system.

Mr. JOHNSON of Georgia. There's no way of doing that—

Ms. JACKSON LEE. The gentleman's time has expired.

Mr. JOHNSON of Georgia. —with the electronic voting process.

I thank the gentlelady, and I yield back.

Ms. JACKSON LEE. The gentleman's time has expired.

The gentleman from North Dakota, Mr. Armstrong, is recognized for 5 minutes.

Mr. ARMSTRONG. Thank you, Madam Chair, if I have time, I am going to come back to this, but Mr. Burt, your written testimony, you mentioned, you talked about future threats, and one of those was deepfakes and synthetic media being a future threat. I'm an old State party chairman. I understand how in the last 10 days of a close election things escalate extremely quickly. Just, why is this such a threat, and what can we do to deal with it on the front end? I mean, I've seen some—our colleagues, they did one yesterday, and I don't know another word to say another than creepy, and they look absolutely legitimate, so.

Mr. BURT. Well, Congressman, that's exactly why it's such a threat. We know that our adversaries, among other things, engage in disinformation campaigns, in which they attempt to take the extreme positions on social issues relevant to the campaign, and they try to incite conflict among the American electorate. They seek to discredit candidates or positions through their disinformation campaigns. We should anticipate that they are going to become more sophisticated in their efforts.

Synthetic media, or deepfakes as it's called regularly, the technology that enables that, both in terms of audio and video, is advancing rapidly, and as you point out, it's now possible, with the most advanced technology, to really create videos that appear to be entirely realistic. There's a lot of research that's going into detection technology, how to detect these deep fake videos and show that they are artificial and not real. At the end of the day, the technology to create the videos, because of the way the artificial intelligence works, will always be ahead of any detection algorithm.

So, the opportunity for our adversaries to use this technology, to try to influence a campaign or an election, is very real. Today as it stands right now, we don't have a great answer to that, other than to educate the American public that it's going to be even more important now than it's been in the past, that they consume the information that they use to make election decisions from sources they believe are credible. There are a number of services out that try to rank and rate various sources to determine is this a journalistically credible source or not, but in today's world, that's going to become even more important.

Mr. ARMSTRONG. Thank you. I get criticized for a lot of things I say, so I'd prefer that I not get criticized by things people make up that I say. Moving into that, as far as a defense to that, as we're going forward, if the technology is advancing faster than the detection of it, it probably behooves us, as a body, and whoever else is doing some of these things, to figure out a way, particularly with platforms and things, to be able to have immediate removal and those types of efforts. Would that probably be just as we're moving forward and going towards this, there has to be a way. We have to have a way as a Congress or as a government or just as an election, to be able to deal with these things.

Mr. BURT. Yes. In the short-term, I think using available detection technologies, working with the social media platforms and others to try to identify those that originate from adversaries, which is, cybersecurity technology we can deploy. Those are going to be the best things we can do for this election cycle.

We and others are investing in a number of different efforts to try to come up with better ways, both to detect and to identify legitimate sources of video and audio so that over time, we will have a better approach to solving this challenge. It is going to be a real challenge for us in the 2020 elections.

Mr. ARMSTRONG. Going back to the encryption stuff, and how does the broader encryption debate potentially affect encryption in ElectionGuard. If a government has a backdoor access, it's a backdoor that potentially could be exploited. That could create a built-in weakness in the balance. How do we balance law enforcement and the ability to do that with cybersecurity?

Mr. BURT. So, this is a broader question that goes beyond the election context. In the election context, the encryption that we build in to ElectionGuard would never have a backdoor. There would be no purpose to have the backdoor, and it actually would reveal voter—specific votes, which you don't want to do for a variety of reasons.

In the more broader context, this is a very nuanced discussion. There was a recent paper from the Carnegie Institute that I thought was very well done in talking about the broad range of issues, relevant to encryption, law enforcement access, protection of dissidents, for example, the legitimate uses for encryption, why that's important. One of the things that paper said, which we absolutely endorse, it's important to get very specific about the problem you're trying to address, and look at that problem and how to properly balance all the competing interests as to that problem. There is no general approach to encryption that doesn't create way too many problems. So, we need to be very specific, look at those specific things, and then balance the social issues to find the right result, and that's going to be some work that we all have to do, the technology industry together with government.

Chairman NADLER. The time of the gentleman has expired. The gentleman from Rhode Island.

Mr. CICILLINE. Thank you, Mr. Chairman. Thank you to our witnesses for this very useful and important testimony. One of the things that I'm particularly concerned about is the regulation of vendors. As you are aware, a large percentage—I think it's 97 percent—of States and territories use vendors in some capacity, from the computers they use to access information to the servers that house information, the management of databases that contain information to cast and tally votes, websites and software used to display information and results, to the software that creates ballot design and helps transfer information across systems.

Three vendors in particular control over 90 percent of this process. Of those three, over 60 percent of American voters cast ballots on systems owned and operated by a single vendor. Despite the incredible impact of vendors on our electoral system, there seems to be very little regulation over vendors that really ensures election

security. As a result of it, we've seen some very serious issues with vendor security.

So, my first question really is, for each of the witnesses, should we consider regulations at the Federal level in creating some standards for vendors, and if so, why? If not, why not?

Ms. PLUNKETT. I absolutely believe that we should, because elections and election systems are a national security threat. For national security threats, that has been the approach of the U.S. Government. It is to develop Federal standards, and in this case, it would be Federal security standards for election equipment that range—that really run the gamut from how the environment in which the software is developed, and ensuring that it's developed in a secure manner, and appropriately protected, straight through to the implementation and maintenance, and then the responsibility for reporting any vulnerabilities that are discovered even after that software, hardware is deployed. I think it absolutely should be done, and I believe it's a role for the Federal Government.

Ms. BOOCKVAR. I agree on every level. We have the Election Assistance Commission which does certification, but as you probably know, not only has the AC been underfunded, but they also were unable to update their standards, the voluntary VBSG standards, for a long time. It didn't have a quorum.

So, for example, in Pennsylvania, we stepped in and last year, when we knew we had to certify a whole bunch more voting systems, we actually created our own more stringent security standards, because we didn't want to rely on the outdated ones.

So, it would be much more effective if the Federal Government were having stronger oversight both to standards and then to oversight of, for example, we talked earlier about the foreign ownership, background checks, and making sure that there's chain-of-custody controls over every component of the voting and election system.

Mr. CICILLINE. To make those standards requirements, not voluntary?

Ms. BOOCKVAR. Correct.

Mr. BURT. Congressman, if I may add, we're all in agreement on that, with the one caveat that it's important that the standards not dictate any particular technology or technological solution because that then sticks the States and local governments with a particular solution. If that becomes vulnerable, then it would take too much time to change. So, they need to be generalized standards so that there can be innovation in terms of the technology approach that's used to meet those standards.

Mr. CICILLINE. That makes sense. In addition to the establishment of mandatory standards, are there other things Congress should be thinking about with respect to the role vendors play in our electoral process and the integrity of our elections?

Mr. BURT. One thing that is another one of the future threats that the vendors can be playing a more significant role is, the risk of ransomware, and ransomware attack, especially on the voter registration rolls. This is something that Director Krebs from CISA pointed out a few weeks ago after this whole rash of ransomware attacks, we've seen on small municipalities around the country, ten

in Texas alone relatively recently. The risk that our adversaries will use that same malware injected into the voter registration devices, and basically it will show up on the day of the election, and the entire database will be locked up and you can't see it. That's a significant risk.

So, vendors need to work with their customers to help them understand how to establish defenses, how to have and build into the system backups that are offline backups, and do tabletop exercises so that State and local officials know how to restore those systems very rapidly, so there's no interruption in the voting process in the event that everything else that we do to try to maintain security is unsuccessful.

Mr. CICILLINE. Thank you. I want to thank you, Mr. Chairman, for holding this really important hearing. There's nothing more fundamental than protecting the right of the American people to have their voices heard and their votes counted in our elections, and this requires strong leadership from everyone at every level of government, and I really thank you for conducting this hearing.

Chairman NADLER. Thank you, the gentleman yields back. The gentleman from Texas.

Mr. GOHMERT. Thank you, Mr. Chairman. I appreciate all of you being here. I noted that Chairman said basically that he was astounded to find counties still buying machines with no paper trail. Ms. Plunkett, were you at the NSA back in 2000, 2001?

Ms. PLUNKETT. Yes, I was.

Mr. GOHMERT. Do you remember who mandated that every county or parish in America buy electronic voting machines, and there was no requirement for paper trails because that was more expensive? Do you remember who mandated that?

Ms. PLUNKETT. No, I do not.

Mr. GOHMERT. Well, I was working for the State and county as a judge, and counties were outraged that they had an unfunded mandate by this Congress, that some people here were in, Democrats intimidated Republicans because of the votes in Florida, even though there were fifth graders tested. None of them had trouble with the butterfly ballots and such. Apparently, people that were trying to vote Democrat had a lot of trouble with them. So, there was outrage, there was demand for electronic voting, and the Federal Government, Congress, mandated it. It was very, very difficult for counties, many counties, to come out of the financial burden that this Congress put on them, and so, if some of them have had trouble recovering financially for the poor mandate from this Congress, then hopefully they will be forgiven.

Mr. Burt, it's wonderful that ElectionGuard is being provided by Microsoft to help secure elections. Does that work as well on Apple or Mac systems as it does on Microsoft operating systems?

Mr. BURT. Yes, Congressman, it works on any platform. It doesn't matter what platform—

Mr. GOHMERT. See, I've heard that about here in Washington, I could have whatever computer system I wanted, and I have used Microsoft operating system for years. I tell people, I thought Microsoft Vista was the best thing that ever happened to computers. It screwed up all my software. I finally got mad and went and bought an Apple, it was a Mac. It was the best thing I ever did. Bought

dozens since. But, when I was in Congress, I wanted a Mac, and I got one, but Microsoft system is what things are based on here. It screwed up my computer, and they said, look, you just can't have a Mac, if you're going to communicate with other computers around it. So, I just didn't know.

I understand that your job is security and trust with Microsoft, so maybe they hadn't told you, but is there any backdoor into ElectionGuard that Microsoft might have in order to fix or deal with some problem in the system?

Mr. BURT. Absolutely not, Congressman. There is no—

Mr. GOHMERT. As far as you know.

Mr. BURT. Well, not only as far as I know, but it was my team that did the engineering work on this ElectionGuard—

Mr. GOHMERT. Okay.

Mr. BURT. —and so, I am confident there is no backdoor. The other thing I would say again is, we are making it an open-source project. So, the source code is available today on GitHub for anybody to look at. We actually encouraged hackers to try to hack into it, so that we can find any security flaws and fix them.

Mr. GOHMERT. One of the problems since really we're all very concerned about election security, no matter how good your system is, it can't do anything about a county that hires a vendor, as my colleague was just bringing up, and the vendor at the end of our early voting, on Friday before the election on Tuesday, takes the 48 flash drives from the 48 precincts home and plays with them until Election Day. Your system can't help with that kind of problem, correct?

Mr. BURT. Actually, Congressman, the ElectionGuard technology, the way it works, actually provides security and trustworthiness even if you have a vendor or an election official who's been compromised or has some malign intent, because the vote gets encrypted the moment that the voter votes on it, and it never decrypts it after that.

Mr. GOHMERT. Yeah.

Mr. BURT. So, it's protected against any of those kinds of attacks. Then we—

Mr. GOHMERT. If it's protected against that kind of abuse, then a county may not want to use your system, if they need a vendor to take them home and play with them. I'm concerned that each of you think it is possible to rig an American election, and if that's the case, I just warn you that in President Obama's eyes, that would make you a nonserious person, because he said, no serious person out there would suggest somehow you could even rig America's elections.

I would encourage you, since traditionally dead people vote nearly a hundred percent Democrat, that you figure out a way to secure our graveyards so people don't keep turning out and voting in our elections. My time is expired.

Chairman NADLER. The gentleman's time is expired. The gentlelady from Washington.

Ms. JAYAPAL. Thank you, Mr. Chairman, and thank you all for being here. It's really very important the information that you're giving to us. As I've come to learn more about this issue, I've been quite stunned that the United States is currently the only major

democracy without a centralized agency governing cybersecurity. Although we have multiple Federal agencies that have some role to play in protecting elections, there's no clear place that a local county that's concerned about hacking can go to. I read this recent U.K. report that explains that there are single, centralized, cybersecurity agencies that coordinate national security in Australia, Canada, and New Zealand, but the same report notes that in the United States international cybersecurity efforts must go through multiple U.S. agencies, including the NSA, DHS, and the FBI. So, I'm really interested in this idea of centralized and cohesive coordination of our Nation's cybersecurity to better protect from foreign and domestic threats.

Mr. Burt, I want to thank you for your work and say how proud I am that Washington State is Microsoft's home State, and that I have the honor of representing many, many, many Microsoft workers as my constituents. I think you have brought up some really—you've done some really important work with the ElectionGuard technology. I'm curious—I know you just released it—is it actually in use anywhere yet? Are we using it in Washington, I guess, is the most relevant question?

Mr. BURT. No, it's not yet in use anywhere, because as you say, just released it for public use just in the last few days. We are working with all the major election—working with all the election vendors. They're all very enthusiastic. They're in the process now of evaluating the technology and thinking about how they could build it into new offerings, new devices. So, we need both the election vendors, as well as State and local officials to understand the technology, think about how they can use it to secure their election, and we're out, you know, actively helping explain and educate that.

We do expect that either later this year, or certainly in 2020, there will be—we're working with a number of partners on some, at least pilot elections, where it will be used for a certain precinct or in a certain location so that we can actually test the technology, make sure that it's working as expected, hopefully in the coming months, and certainly by 2020.

Ms. JAYAPAL. Thank you. That's what I was wondering, is perhaps if we were pilot-testing it in Washington. In your testimony, you talked about imposing a culture of cybersecurity, including training, and I was also struck by the fact that many of the existing voting systems were using Windows 7. In your testimony you talked—or in your written statement, you talked about that. How do we, and maybe this is a question for you, but also for you, Ms. Boockvar, how do we make sure that we are providing the support and incentivizing in some way States and local counties to update their technology? Because we can have the best stuff, and we can put it out there, but if people don't continue to update, we're going to have this problem. Do either of you have comments on that?

Mr. BURT. Well, I think you've heard a number of comments that address that already today from the testimony. I would say, we basically endorse the comments from both other witnesses which is, among other things, a set of consistent Federal standards on security for elections would be useful guidance. But, you also need to have a sustained, durable, long-term funding solution, so that State and local agencies are not stuck because of financial considerations,

with outdated technology. This is just too important to our democracy. We need to make sure that we have the most secure systems possible in every State and local elections.

Ms. JAYAPAL. Is it just about money, though, or is it also about people's fear of how to use technology, not perhaps having their technology officers in place? Either of you, please.

Ms. BOOCKVAR. There's a role really for lots of different pieces of the puzzle here, so from—everything from—sorry about that. We were talking earlier about how it would have been great if the new systems, for example, in Pennsylvania, that we just certified over the last year, they should—it would have been great if they were never made with Windows 7, so that there was an earlier sort of prevention measure in place that just involves regulation at the front end.

Then, I think at the county level, and at the State level, and at the Federal level, to have easier certification, so when there is the transition and the upgrade of technology, we need to be able to make sure that those systems can be in use without being out of play for a while. So, there's a lot of different levels of it.

Ms. JAYAPAL. You mean made with Windows 7, because things have an operating system within them, but what do you mean by that?

Ms. BOOCKVAR. So that's their operating system B. So, for example, it would have been great if all the systems that were even being made over the last year were already Windows 10. Some were, some weren't.

Ms. JAYAPAL. Oh, I see. I see. They were updated as they were being put out?

Ms. BOOCKVAR. Correct. The counties, so there were negotiations—in terms of the money piece, there were negotiations with the vendors to make sure that they weren't going to charge for the upgrade, but it would have been better if there was never a need for upgrade because they had been made with Windows 10 to begin with.

Ms. JAYAPAL. Thank you. I yield back.

Chairman NADLER. The gentlelady yields back.

The gentleman from Virginia.

Mr. CLINE. Thank you, Mr. Chairman, and I'm grateful to you for holding this hearing today. It's an issue that has needed examination for some time, and I'm hopeful that after today's hearing, we'll be able to Act on some of the excellent ideas that have been discussed this morning and many others that have been put forward by Members on this committee.

While the responsibility of carrying out elections is one mainly for local and State governments, the Federal Government does have a critical role to play as has been discussed. It's a fact that other countries are trying to interfere in U.S. elections—Russia, most notably—and we must remain vigilant to ensure that foreign adversaries cannot mettle in our electoral process.

New threats will never cease, and our Nation must stay on the cutting edge to ensure our elections remain secure. Our laws guarantee the American people just and fair elections, and it's our duty to carry out that mandate and resist all forms of tyranny that threaten our freedom.

I have listened with interest. It seems like we're moving in two different directions—one toward less technology, paper ballots, and one toward more use of technology, decentralization, Blockchain. I'm curious about real-time testing of Blockchain in West Virginia.

Ms. Boockvar, your neighboring State, West Virginia, had apparent success in the midterms in using Blockchain to allow deployed overseas servicemembers to vote. Have you explored any similar initiatives in Pennsylvania, and what have you done to ensure that overseas, deployed servicemembers can vote?

Ms. BOOCKVAR. So, we have not explored directly—I think across the country we are very closely talking with Virginia and West Virginia and watching how this goes. I think it did seem that the first run of it was successful. But, like we all know, there's a lot of risks with using untested technology. So, I think that's going to be something to watch over time. In the meantime, we are effectuating an encrypted email process that's going to be used for the first time—I'm sorry, I lost my voice—but that's going to be used, that's going to allow, instead of having to access a website, encrypted emails for delivery of the ballot to those voters, and that's kind of our next technology way to protect the vote overseas—of overseas voters. I'm sorry.

Mr. CLINE. Mr. Burt, your technology seems to—ElectionGuard seems to utilize both ends of the spectrum there. You're having a paper ballot backup but exploring open-source solutions. Do you still—are you researching efforts to replace paper ballots, design and create additional software efforts that could replace paper ballots? Or are you of the mind that you should always have that paper ballot backup?

Mr. BURT. So, our view is that whether paper ballot is the backup or primary, either way, the ElectionGuard technology can help provide this level of security and verifiability. We've designed it so that it will work with paper ballots in either way. But our position is that today, it's important to have a verified paper ballot backup, at a minimum, to use for risk-limiting audits and have it available in the worst case, so that you can do a hand count if necessary. So, we think—and our technology supports that as well—so we think it's important.

If I just make comment quickly on Blockchain, our researchers, who look really carefully at election-based technology, do not think Blockchain is a great solution for a nationwide election. We're very interested in the West Virginia experiment. We'll continue to look at that. It has a very specific focus which it may be useful for. For the most part, there are two big problems with Blockchain. It's a distributed ledger, and you really need to have a leader, which we have leaders now with the State and local election officials who establish what the rules are for voting and for who's on the ballot and who's not. So, there's challenges with Blockchain technology inherently, and furthermore, on a nationwide level, it would not maintain the degree of security and privacy in each individual's vote that is critical to our national elections.

Mr. CLINE. You've been working globally on this effort. Have you seen in other countries any evidence of hackers and whether your work in other countries on those issues has led directly to denying hackers an option to penetrate election infrastructure?

Mr. BURT. So, the work that we've done globally so far has been with our account guard service, where we monitor Nation State actors, attempting to hack into the accounts of candidates or others involved in the election process, including third-parties, academics, and NGOs. What we have seen is that there are attacks in many other countries. We saw it in a number of the ones that Chairman Nadler referenced in his opening statement. We saw it as well in the French presidential election following ours in 2016. So, this pattern of conduct by the Russians, but potentially by other nation-states, is absolutely continuing in multiple different countries.

Mr. CLINE. I thank the witnesses.

Chairman NADLER. The time of the gentleman is expired. The gentleman from Maryland.

Mr. RASKIN. Mr. Chair, thank you. In 2016, Vladimir Putin assessed the Russian posture vis-à-vis other countries. He realized he could not defeat liberal democracies militarily or economically, but he convened the equivalent of a Manhattan project for electronic subversion of the cyber elections, and the social media of Democratic countries.

So, from prior hearings I've learned it was a three-pronged attack. Part of it was on the social media. There was an effort to inject racial propaganda and other kinds of ideological poison into Facebook and Twitter and so on. Two, there was a direct effort to hack into the DNC, at the D triple C, Hillary Clinton's emails. We're aware of that and had testimony about that.

The third part was to go right to the State boards of elections to try to get into those systems. I want to ask a couple questions about that. I understand that they made their most progress in terms of the Illinois system, actually got into the voter registration database. Although, they were not able to, but apparently they tried, but they were not able to nullify the existence of voters on the database. What might have happened had they been able to do that? How secure are we against that in a similar attack, in 2020, Ms. Boockvar?

Ms. BOOCKVAR. So, the way it's been described to me is, what they did was kind of like, you know, if you're a thief and you go around the neighborhood and you try to figure out which houses have unlocked doors or windows, which are the easiest to break into, and when they're locked, you move on to the next one. So, they scanned a bunch of States, found most of the doors and windows locked and moved on to the next. I think that that's why we were successful at not having a worse situation. It could have been, as has been discussed previously, it could have been devastating.

Mr. RASKIN. Are you a member of the National Association of Secretaries of State?

Ms. BOOCKVAR. Correct.

Mr. RASKIN. How secure are the States? How ready are we? People ask me all the time, how ready are we, but we don't have one system. We have at least 50 systems, right? Or 51 systems all over the country.

Ms. BOOCKVAR. I think we are absolutely in a much better place than we were 2 years ago, and the designation of elections as critical infrastructure was a big start to that. We still have a way to go, and that's why I'm really interested, Congressman, on making

sure that we don't focus entirely on voting systems. Voting systems are really important, but we need to be funding replacement of voter registration systems, intrusion-detection systems, making sure that the counties have the cyber protections, the passwords, and the multifactor authentication. Those are just as important as the voting systems, and we need to recognize that.

Mr. RASKIN. Ms. Plunkett, would we be safer in protecting our Presidential elections, which are obviously the biggest magnet and target for foreign actors, would we be better off if we had one national popular vote in electoral system for President, or are we better off using the current electoral college system where we have a State-by-State voting and we've got to protect all those different systems?

Ms. PLUNKETT. What's most important is that we have the right—whichever system we would choose to use, what's most important is that we have the right security protections in place. With the right security protections in place, either would work equally effectively, I believe.

Mr. RASKIN. Okay. Mr. Burt, I was very cheered to hear your testimony. Are you telling us that we essentially have a technological fix to the problem of security of the actual voting systems themselves?

Mr. BURT. Yes, Congressman. We think the election, our technology, once it's implemented in devices and those devices have been adopted, will provide a high degree of security, and more importantly, will provide this end-to-end verifiability, which will enable individual voters and voting officials to be able to trust the outcome, with the ability to have audits as a backup to add a layer of verifiability and trust in the system.

Mr. RASKIN. It will promote a lot more confidence in the reliability of the results?

Mr. BURT. Yes. Ultimately, it would provide a much greater degree of confidence in the outcome, in part, because individual voters, for the first time, will see that their vote actually was counted.

Mr. RASKIN. Yeah. I mean, all of you have emphasized that our electoral integrity is a matter of national security. If you think about it, why does Vladimir Putin and Prime Minister Orban in Hungary and Duterte and all the authoritarians and despots and dictators want to destabilize our elections, it's because they want to destroy people's faith and confidence in democracy. They would like everything to be about authoritarian despots who just make deals around the world and go and corrupt each other's elections and interfere in each other's governments. I yield back. Thank you for your testimony.

Chairman NADLER. The gentleman yields back. The gentleman from Pennsylvania.

Mr. RESCHENTHALER. Thank you, Mr. Chairman.

Mr. Burt, thanks for coming in today, and thanks for all you're doing to make our elections safe and protecting democracy. I just wanted to see if you'd like to speak about why Microsoft got into the election space and just generally speak, say, if there's anything more you want to elaborate on ElectionGuard.

Mr. BURT. Absolutely. This goes to a number of the questions about how we got to where we're at today. We need to keep in mind

that our foreign adversaries' direct efforts to intervene in our elections is a relatively new phenomenon, and the process for certifying devices and so forth is an older phenomenon. So, this is something that the entire election community is reacting to in a relatively short period of time.

For Microsoft, this started in 2016, during the Democratic National Convention when our security team saw that a group that we call STRONTIUM, which we now know from the Mueller indictment, is a Russian organization operated by the GRU, the same group. When we saw that organization registering a bunch of fake Microsoft domains, domain names, websites that looked like they were Microsoft, but really were not, and because of the timing, we immediately took action, and ultimately, actually, went to court. We've been in a battle with that same organization now over several years in court, where every time they register fake domains, or use them to try to steal credentials, we go to court, get an order, we take those down and direct all of that traffic to our own sinkhole at our digital crime's unit. So, we're in a constant technological battle with that organization. It started then.

Then as we fast-forward over the next year, I had a conversation with our president, my boss, Brad Smith, and we talked about the obligation we have as a company, a company based in a democracy, founded in a democracy, to help protect, however we can, those democratic institutions and our voting process as a core democratic institution. That's when we founded our Defending Democracy Program which we're going to continue to invest in and advance in coming years.

Mr. RESCHENTHALER. Thank you again, Mr. Burt. I really appreciate all you're doing, and with that, I would yield the remainder of my time to my friend and colleague from Florida.

Mr. GAETZ. I thank the gentleman for yielding. Mr. Chairman, I initially have a unanimous consent request that H.R. 3529, the bipartisan election security legislation I referenced earlier be entered into the record.

Chairman NADLER. Without objection.

[The information follows:]

MR. GAETZ FOR THE RECORD

I

116TH CONGRESS
1ST SESSION

H. R. 3529

To require the Secretary of Homeland Security to promptly notify appropriate State and local officials and Members of Congress if Federal officials have credible evidence of an unauthorized intrusion into an election system and a basis to believe that such intrusion could have resulted in voter information being altered or otherwise affected, to require State and local officials to notify potentially affected individuals of such intrusion, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JUNE 27, 2019

Mrs. MURPHY (for herself, Mr. WALTZ, Ms. SHALALA, Mr. SOTO, Mr. FITZPATRICK, Ms. KENDRA S. HORN of Oklahoma, Mr. GAETZ, Mr. DEUTCH, Mr. SPANO, Ms. MUCARSEL-POWELL, Mr. MAST, Ms. WASSERMAN SCHULTZ, Mr. DIAZ-BALART, Mr. CRIST, Mr. RUTHERFORD, Mr. ARRINGTON, Mr. BUCHANAN, and Mr. YOHO) introduced the following bill; which was referred to the Committee on House Administration

---

A BILL

To require the Secretary of Homeland Security to promptly notify appropriate State and local officials and Members of Congress if Federal officials have credible evidence of an unauthorized intrusion into an election system and a basis to believe that such intrusion could have resulted in voter information being altered or otherwise affected, to require State and local officials to notify potentially affected individuals of such intrusion, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Achieving Lasting Electoral Reforms on Transparency and Security Act'' or the ''ALERTS Act''.

SEC. 2. FINDINGS; SENSE OF CONGRESS.

(a) FINDINGS.—Congress finds as follows:

(1) Free and fair elections are central to our democratic system of government.

(2) An attack on election systems in the United States by a foreign government is a hostile act, and protecting our election systems from such attacks is a critical national security objective.

(3) The March 2019 ''Report on the Investigation into Russian Interference in the 2016 Presidential Election'', known as the Mueller Report, concludes that Russian military intelligence officers targeted individuals and entities involved in the administration of the November 2016 elections, including State boards of elections, Secretaries of State, county governments, and private technology firms responsible for manufacturing and administering election-related software and hardware.

(4) The Mueller Report states that Russian military intelligence officers sent spearphishing emails to over 120 email accounts used by Florida county officials responsible for administering the 2016 elections, and further states that the Federal Bureau of Investigation ''believes that this operation enabled Russian military intelligence officers to gain access to the network of at least one Florida county government''.

(5) In May 2019, it came to light that Russian military intelligence officers had gained access to the computer network of a second Florida county in the run-up to the 2016 elections.

(6) To date, government officials have not publicly disclosed or confirmed the identity of the Florida counties whose voter registration systems were breached.

(7) As a result, voters in affected counties do not possess the information necessary to take appropriate responsive action, such as taking affirmative steps to confirm that their individual registration data is accurate and holding State and local election officials accountable for their actions or inactions.

(b) SENSE OF CONGRESS.—It is the sense of Congress that the principal victim of an attack on election

systems in the United States is the voting public and, except in certain narrowly defined cases, the voting public should be promptly informed if Federal officials have credible evidence of an unauthorized intrusion into an election system and a basis to believe that such intrusion could have resulted in voter information systems or voter tabulation systems being altered or otherwise affected.

SEC. 3. DEFINITIONS.

In this Act, the following definitions apply:

(1) APPROPRIATE MEMBERS OF CONGRESS.—The term ''appropriate Members of Congress'' means, with respect to a notification described in section 3(b)(2)—

(A) the Speaker of the House of Representatives, the Minority Leader of the House of Representatives, the chairs and ranking minority members of the Committees on House Administration, Homeland Security, the Judiciary, and Permanent Select Committee on Intelligence of the House of Representatives, and each Member of the House of Representatives (including a Delegate or Resident Commissioner to the Congress) who represents a congressional district in which the unit of local government involved is located; and

(B) the Majority Leader of the Senate, the Minority Leader of the Senate, the chairs and ranking minority members of the Committees on Rules and Administration, Homeland Security and Governmental Affairs, the Judiciary, and Select Committee on Intelligence of the Senate, and the Senators who represent the State involved.

(2) DEPARTMENT.—The term ''Department'' means the Department of Homeland Security.

(3) ELECTION AGENCY.—The term ''election agency'' means any component of a State or any component of a unit of local government of a State that is responsible for administering Federal elections.

(4) ELECTION CYBERSECURITY INCIDENT.—The term ''election cybersecurity incident'' means any incident, as defined in section 2209(a)(3) of the Homeland Security Act of 2002 (6 U.S.C. 659(a)(3)), involving an election system.

(5) ELECTION SYSTEM.—The term ''election system'' means a voting system, an election management system, a voter registration website or database, an electronic pollbook, a system for tabulating or reporting election results, an election agency com-

munications system, or any other information system (as defined in section 3502 of title 44, United States Code) that the Secretary identifies as central to the management, support, or administration of a Federal election.

(6) FEDERAL ELECTION.—The term ''Federal election'' means any election (as defined in section 301(1) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101(1))) for Federal office (as defined in section 301(3) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101(3))).

(7) FEDERAL ENTITY.—The term ''Federal entity'' means any agency (as defined in section 551 of title 5, United States Code).

(8) LOCAL ELECTION OFFICIAL.—The term ''local election official'' means the chief election official of a component of a unit of local government of a State that is responsible for administering Federal elections.

(9) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(10) STATE.—The term ''State'' means each of the several States, the District of Columbia, Puerto Rico, Guam, American Samoa, the Commonwealth

of the Northern Mariana Islands, and the United States Virgin Islands.

(11) STATE ELECTION OFFICIAL.—The term ''State election official'' means—

(A) the chief State election official of a State designated under section 10 of the National Voter Registration Act of 1993 (52 U.S.C. 20509); or

(B) in the case of Puerto Rico, Guam, American Samoa, the Northern Mariana Islands, and the United States Virgin Islands, a chief State election official designated by the State for purposes of this Act.

(12) VOTING SYSTEM.—The term ''voting system'' has the meaning given the term in section 301(b) of the Help America Vote Act of 2002 (52 U.S.C. 21081(b)).

SEC. 4. DUTY OF SECRETARY OF HOMELAND SECURITY TO NOTIFY STATE AND LOCAL OFFICIALS AND APPROPRIATE MEMBERS OF CONGRESS OF UNAUTHORIZED INTRUSIONS INTO ELECTION SYSTEMS.

(a) DUTY TO SHARE INFORMATION WITH DEPARTMENT OF HOMELAND SECURITY.—If a Federal entity receives information about an election cybersecurity inci-

dent, the Federal entity shall promptly share that information with the Department, unless the head of the entity (or a Senate-confirmed official designated by the head) makes a specific determination in writing that there is good cause to withhold the particular information.

(b) RESPONSE TO RECEIPT OF INFORMATION BY SECRETARY OF HOMELAND SECURITY.—

(1) IN GENERAL.—Upon receiving information about an election cybersecurity incident under subsection (a), the Secretary, in consultation with the Attorney General and the Director of National Intelligence, shall promptly (but in no case later than 96 hours after receiving the information) review the information and make a determination whether each of the following apply:

(A) There is credible evidence that an unauthorized intrusion into an election system occurred.

(B) There is a basis to believe that the unauthorized intrusion resulted, could have resulted, or could result in voter information systems or voter tabulation systems being altered or otherwise affected.

(2) DUTY TO NOTIFY STATE AND LOCAL OFFICIALS AND APPROPRIATE MEMBERS OF CONGRESS.—

(A) DUTY DESCRIBED.—If the Secretary makes a determination under paragraph (1) that subparagraphs (A) and (B) of such paragraph apply with respect to an unauthorized intrusion into an election system, not later than 48 hours after making the determination, the Secretary shall provide a notification of the unauthorized intrusion to each of the following:

(i) The chief executive of the State involved.

(ii) The State election official of the State involved.

(iii) The local election official of the election agency involved.

(iv) The appropriate Members of Congress.

(B) TREATMENT OF CLASSIFIED INFORMATION.—

(i) EFFORTS TO AVOID INCLUSION OF CLASSIFIED INFORMATION.—In preparing a notification provided under this paragraph to an individual described in clause (i), (ii), or (iii) of subparagraph (A), the Secretary shall attempt to avoid the inclusion of classified information.

(ii) PROVIDING GUIDANCE TO STATE AND LOCAL OFFICIALS.—To the extent that a notification provided under this paragraph to an individual described in clause (i), (ii), or (iii) of subparagraph (A) includes classified information, the Secretary (in consultation with the Attorney General and the Director of National Intelligence) shall indicate in the notification which information is classified.

(3) EXCEPTION.—

(A) IN GENERAL.—If the Secretary, in consultation with the Attorney General and the Director of National Intelligence, makes a determination that it is not possible to provide a notification under paragraph (1) with respect to an unauthorized intrusion without compromising intelligence methods or sources or interfering with an ongoing investigation, the Secretary—

(i) shall not provide the notification under such paragraph; and

(ii) shall, not later than 48 hours after making the determination under this subparagraph, provide a classified briefing

on the unauthorized intrusion to the appropriate Members of Congress.

(B) ONGOING REVIEW.—Not later than 30 days after making a determination under subparagraph (A) and every 30 days thereafter, the Secretary shall review the determination. If, after reviewing the determination, the Secretary makes a revised determination that it is possible to provide a notification under paragraph (2) without compromising intelligence methods or sources or interfering with an ongoing investigation, the Secretary shall provide the notification under paragraph (2) not later than 48 hours after making such revised determination.

(c) EFFECTIVE DATE.—This section shall apply with respect to information about an election cybersecurity incident which is received on or after the date of the enactment of this Act.

SEC. 5. RESPONSIBILITIES OF STATE AND LOCAL OFFICIALS TO NOTIFY AFFECTED INDIVIDUALS.

(a) RESPONSIBILITIES DESCRIBED.—Title III of the Help America Vote Act of 2002 (52 U.S.C. 21081 et seq.) is amended by inserting after section 303 the following new section:

"SEC. 303A. RESPONSIBILITIES OF STATE AND LOCAL OFFICIALS TO NOTIFY INDIVIDUALS AFFECTED BY UNAUTHORIZED INTRUSIONS INTO ELECTION SYSTEMS.

"(a) RESPONSIBILITIES DESCRIBED.—If a State or unit of local government receives a notification from the Secretary of Homeland Security under section 4 of the Achieving Lasting Electoral Reforms on Transparency and Security Act of an unauthorized intrusion described in such section, the State election official and the appropriate local election official shall provide notification of the intrusion to the individuals who were affected, could have been affected, or may be affected by the intrusion.

"(b) CONTENTS AND MANNER OF NOTIFICATION.—The notification provided under this section shall be in such form and manner as the State election official may establish, except that—

"(1) the notification shall not reveal classified information about the nature of the intrusion or the persons suspected of making the intrusion;

"(2) the notification shall be provided in a manner that does not discourage any individual from voting or registering to vote; and

"(3) nothing in this section shall be construed to require an election official to provide a separate notification to each affected individual.

''(c) DEADLINE.—The State election official or the appropriate election official shall provide the notification required under this section as soon as practicable after the official receives the notification from the Secretary of Homeland Security under section 4 of the Achieving Lasting Electoral Reforms on Transparency and Security Act, but in no event later than—

''(1) 48 hours before the date of the next election for public office held in the State or unit of local government involved; or

''(2) 30 days after receiving the notification,

whichever is earlier.

''(d) DEFINITIONS.—In this section, the terms 'State' and 'State election official' each have the meaning given such term in the Achieving Lasting Electoral Reforms on Transparency and Security Act.''.

(b) CONFORMING AMENDMENT RELATING TO ENFORCEMENT.—Section 401 of such Act (52 U.S.C. 21111) is amended by striking ''sections 301, 302, and 303'' and inserting ''subtitle A of title III''.

(c) CLERICAL AMENDMENT.—The table of contents of such Act is amended by inserting after the item relating to section 303 the following new item:

''303A. Responsibilities of State and local officials to notify individuals affected by unauthorized intrusions into election systems.''.

○

Mr. GAETZ. Thank you. I want to return to this issue of paper ballots versus blockchain technology, and I know that we all likely have a lot to learn on that. Mr. Burt, do you view blockchain technology as potentially being more applicable to the voter rolls and the maintenance of the rolls and ensuring that there is no manipulation of those than to the actual vote itself? Or would you view the technology as applicable or inapplicable to those two silos of election data separately?

Mr. BURT. So, I think you do need to evaluate those two things separately, because they really are different problem sets, right? So, you need to look at the problem set and what you're trying to address. There's two different problem sets between voting, where we don't think blockchain is a great solution for a nationwide election, and the voter registration rolls where, to be honest, it's something I need to go back and talk to our experts about, whether it's a potential solution.

Offhand, I'm not sure that it is, because again, you don't really want in the context even of a voter registration roll, you don't want a distributed ledger. You want a ledger with a leader.

Mr. GAETZ. Why is that?

Mr. BURT. Because you want to have someone who has the decision-making authority about what's a legitimate registration and what's not. In a distributed environment, that's being determined by every other participant in that environment. Now, there may be a way to make blockchain applicable to the voter registration process to help with this security issue. I want to go back and talk to our experts. Offhand, I think it's probably not the right technological fit.

Mr. GAETZ. Again I'm not asserting that it is, it's just very interesting to me that it seems to be less susceptible to manipulation because in the event that you had the circumstance you describe, where someone was attempting to manipulate the data, instead of us relying on one supervisor of elections, a Department of State, or even some of these joint task forces that I think we've very productively discussed today, you would have potentially thousands of different nodes and capabilities to be able to diagnose that manipulation.

My concern now is, if you can essentially flummox a supervisor of elections, you can manipulate the voter rolls. As I sit here today, having received the briefing that I know my Florida colleagues received, I'm not certain that in my State, there wasn't some manipulation of the voter rolls. No one's been able to reflect that certainty than me, and so I'm just trying to kind of democratize the oversight of that system, potentially. So, again, I don't expect anyone to be an expert on this. I think we've got a lot to learn about it. I just reject the premise that only a piece of paper gives us a sense of a lack of manipulation.

Mr. BURT. I don't disagree with that, Congressman. If I may, I'd like to go back and—

Chairman NADLER. The gentleman's time is expired. The witness may answer the question.

Mr. BURT. Thank you, Chairman. Let me go back and we come back to you and answer the question more specifically about

blockchain and voter registration rolls, whether that or some other approach is the best means of securing those rolls.

Mr. GAETZ. Thank you. I yield back.

Chairman NADLER. The gentleman yields back. The gentlelady from Florida.

Mrs. DEMINGS. Thank you so much, Mr. Chairman. Thank you to all our witnesses for being here. I am from Florida, and I represent Florida, and I do agree with my colleague's earlier statement from Florida that every voter, regardless of their party, where they live, their zip code, deserves to have their vote counted. So, thank you very much, Mr. Chair, for this very timely and important hearing.

Mr. Burt, I'd just like to ask you, have you faced any obstacles at the Federal level with implementing ElectionGuard, and if so, what have they been?

Mr. BURT. We have not faced any obstacles at the Federal level to implement ElectionGuard. Now that the technology is actually out and available for inspection and deployment, we expect to have continued conversations with a number of representatives, Federal Government, where we will explain the technology and how it works. I don't anticipate actually any Federal-level resistance because, I think we are aligned with the Federal interest, especially those of CISA and others responsible for our election security.

Mrs. DEMINGS. If you could State again, what's the timeline of implementation?

Mr. BURT. So, the technology is available right now for implementation in devices. The timeline is complex, and that is a bit of a problem. It's complex for a number of reasons, some that really government can't do much about, because the vendors have to inspect the technology, determine whether they want to put it in devices. There must be a demand from State and local vendors for the technology, which we think there will be, based on our conversations so far. Then once those are available, there has to be the funding at the State and local level to be able to deploy the new devices that implement the technology, and all of that is subject to this currently outdated certification process that takes too long, it's too burdensome, and it's too hard.

Those rules are being updated right now by the Election Assistance Commission, but we need to make sure they're updated in a way that provides much more agility and flexibility. So, you've got all of those pieces that need to come into alignment. We're confident they will. We're confident we'll have some pilot elections utilizing this technology no later than 2020, but the sooner that it can be deployed to secure our elections, the better.

Mrs. DEMINGS. My understanding is that certain of the breaches in the 2016 election, when they were going door to door looking to see which windows were unlocked, and doors, were not immediately detected. So, my question is, what signs should election officials be trained to look for on election day, to ensure that there are no undetected attacks? Either of—

Ms. PLUNKETT. The first and most important is to have a baseline of what normal looks like. Every election jurisdiction needs to know what normal operations looks like. So that they can then have the appropriate monitoring in place, should there be any ab-

normal activity, whether that be a flow of data that looks unusual, a disruption of data that looks unusual, a login from an unusual—someone who should not have access, from an account that should not have access. So, knowing what normal and having that baseline, and then being able to monitor for any abnormal activity is the most important.

Mrs. DEMINGS. Thank you.

Ms. BOOCKVAR. I would say, every level needs to be trained in this. Starting from technology, right, the intrusion-detection systems should be in every single county in the country and every municipality that runs elections, I think that is one of the most critical components for protecting our elections from here forward. I'd love to see resources from the Federal Government to make sure that happens, so that we don't have voters in under-resourced counties with less security than others.

Then poll workers, my first job in elections was as a poll worker, making sure that we had the support and training for the poll workers to be able to recognize, not only signs that are problematic, like people not being in the voting rolls, but knowing about provisional ballots. We haven't mentioned provisional ballots yet once in this hearing. We actually have a provision that allows when people are not in the voter rolls to still vote. Sometimes poll workers don't remember to do that, or don't know to do that.

So, they need to be adequately trained. Every voter can get a provisional ballot, and then it can be checked later. So, if that person is eligible, they should never, ever be turned away.

Mrs. DEMINGS. Thank you so much.

I yield back, Mr. Chair.

Chairman NADLER. The gentlelady yields back. There are 4 minutes and 20 seconds left on a vote on the floor. We have a number of votes on the floor. The Committee will stand in recess but will reconvene immediately upon cessation of the votes on the floor. So, please, I ask the Members of the committee, come back as soon as the last vote is cast. The Committee stands in recess.

[Recess.]

Chairman NADLER. The Committee will come to order.

The gentlelady from Texas is recognized.

Ms. GARCIA. Thank you, Mr. Chairman.

Thank you for the patience of our witnesses as they waited for us while we registered our votes, and that's what we're focusing on, aren't we, voting. So, thank you for being here.

Election security is all about voter confidence and participation. The more confident voters are in the integrity of our election systems, the more confident they will feel that their vote has been counted and that their voice has been heard and, of course, this directly impacts their future participation.

I listened with great interest to some of your testimony, and I've looked at your written testimony. I wanted to start with you, Mr. Burt. Quickly, I don't need a—I heard you explain the system that you have, and I just want to make sure that anyone watching is clear. Is yours a software system or a software system and machines and an auditing system too or all the above, one of the above?

Mr. BURT. Ours is a software system that needs to be incorporated into the voting system that is utilized by the State or local voting officials, and it supports multiple different forms of voting systems. So, you can have an electronic ballot-marking device. You can start with hand marked ballots that are then scanned. We support those, and we're working to support others that are not as widely used. But, it's basically software that needs to be incorporated by vendors into the voting system itself.

Ms. GARCIA. The verification that the user can—the voter can go to online, that will simply just verify that they voted, or can they print something at home through your software system?

Mr. BURT. So, the system, when they vote, when they go to a polling place and they vote, they get a piece of paper that has the code. They can then enter the code in later and they will see, they will get verification that their vote was counted. They can't see their vote. This is really critically important. They can't see who they voted for. They know who they voted for, but what the system tells them is your vote was not changed and your vote was counted. It's important that they not be able to see their vote, because otherwise, they could be coerced into voting in a certain way, you could sell your vote. This is an important character—

Ms. GARCIA. Anyone doing an audit would also not be able to see how they voted?

Mr. BURT. That's correct. That's actually—

Ms. GARCIA. So there really is no paper trail?

Mr. BURT. There is a paper trail in the sense that our system supports the creation of a verified paper ballot. So, you vote, that's encrypted, but you also get a paper ballot that the voter can look at and say, yes, this is correct. You deposit that in the ballot box. That can be used for risk-limiting audits, even for hand counts, if necessary, although it shouldn't be necessary.

Ms. GARCIA. Well, I'm thinking of a lot of people in my district that don't have a computer at home, don't have a laptop, don't have a way of doing any of that. So, what are we to do with, quite frankly, the usual targeted populations when there are some of this misinformation hacking? It's usually many times, minority voter precincts that get attacked. So, what would we do then for the person who doesn't have access to a computer or internet to be able to go through that process?

Mr. BURT. So, our system is based on polling place voting, whether it's hand-marked ballots or using an electronic voting machine. The election guard supports going to the polling place to vote. So, you don't need to have any technology in order to vote—

Ms. GARCIA. No, but to verify—

Mr. BURT. But to verify and—yes. So—

Ms. GARCIA. I'm talking specifically about verifying that you voted.

Mr. BURT. Correct.

Ms. GARCIA. It's actually sort of happened to me once. I voted and I thought I had done everything, and then they came to the car to get me and said, I was a senator at the time, they said, Senator, it didn't go through. I said, what do you mean it didn't go through? So, I had to go back in and, essentially, vote again. It

made no sense to me that I had to do that. I think that happens probably more often than not.

So, I'm just concerned about the populations who don't have access to their computer to verify that, in fact, their vote was counted.

Mr. BURT. Totally understandable. The good news is that you can do the verification in our system with a smartphone. In most populations, smartphones have penetrated much further than laptops.

Ms. GARCIA. Well, many in my district do not have smartphones. They just have the one that you go to the flea market or a store—what are they called? The click-it phones or flip phones. They don't have a smartphone. Those are more costly. They go in there—Cricket phones. They go there and get 1 month at a time. We're talking about people that are paycheck to paycheck. They can't afford one like mine.

Mr. BURT. Yes. I understand, Congresswoman. The verification does require some access to a system, whether it's your neighbor's phone, your phone, go to the library and access a computer, to get that personal verification. Now, keep in mind, that's a new advance of the technology, but to do that verification and see that your vote was counted, with our system, you will need access to something, whether it's a smartphone, a public computer, some device that lets you see, yes, my vote, in fact, got counted.

Ms. GARCIA. Well, thank you.

I've run out of time and I yield back. Thank you, Mr. Chairman.

Chairman NADLER. The gentlelady yields back.

The gentlelady from Pennsylvania.

Ms. SCANLON. Thank you very much.

Ms. Boockvar, I wanted to thank you for your work in removing barriers to voting in Pennsylvania for everyone who's eligible to vote. In particular, I wanted to thank you for your attention to modernization of Pennsylvania's voting system and things such as, just 2 weeks ago, rolling out the ability to request absentee ballots online. I know my three children, who do not live in the district anymore, when they're at school, appreciate that ability.

You've also paid a lot of attention to our young voters, and I know particularly high school registration. Can you just tell us a little bit about what you've done there?

Ms. BOOCKVAR. Governor Wolf started a couple years ago the Governor's Civic Engagement Award, and it's been a tremendous success in Pennsylvania encouraging students in schools to register eligible voters to vote. It's been terrific, both the competition from school to school and from student to student, but also their engagement in voting, which as we all know—probably a lot of us started our civic engagement early, and it really—research shows when you are engaged early, you probably become life-long voters, and that's critical to our democracy.

Ms. SCANLON. Okay. Turning more to what's at hand here, there's been discussion about needing to improve lines of communication between Federal, State, and local agencies. Can you explain a little bit about that?

Ms. BOOCKVAR. Absolutely. So, one of the things that we've been talking about a lot, and as we've developed these conversations around election security, is the importance of continuity of oper-

ations, or COOP planning. It's one of those things that I think a lot of areas like emergency management and law enforcement have been doing for a long time, but the elections sphere, it's relatively new. One of the critical components of effective COOP planning is to know who to call at the moment you need to call them. Because the last thing you want to do when an incident happens is figure out who the right person is to call.

So, the more clarity we have about who at the Federal Government is the call to make at incident X, Y, or Z, the better it would be for the counties to not to have to figure it out at the moment. We're doing a lot of work with the counties to develop those COOP plans, but we need that to come from the Federal Government as well to make sure we have centralized lines of contact.

Ms. SCANLON. Okay. If you have one piece of advice for Congress as we debate the appropriate vehicles to legislate and to fund this, what would that be?

Ms. BOOCKVAR. I'd have to go back to our conversation about diversifying the types of election security that's implemented across the country. So, there's been a lot of attention to voting systems, which is a very important thing, to transition to paper records. As we discussed earlier, so many other components of this process are at least as critical. So, we need to allow funding to go to voter registration databases, intrusion detection systems, making sure that we have layered defenses to all our networks, phishing and security training and multifactor authentication, and COOP planning. All those things are equally important, and I'm most worried about thinking that one solution is going to fix everything. We need to give the States the ability to decide what their most critical components are.

Ms. SCANLON. As I understand it, that involves both work and helping establish best practices that the Federal Government can help push out and then providing funding to achieve those best practices?

Ms. BOOCKVAR. Exactly.

Ms. SCANLON. Okay. Thank you.

I yield back.

Ms. BOOCKVAR. Thank you.

Chairman NADLER. The gentlelady yields back.

The gentleman from Arizona.

Mr. STANTON. Thank you, Chairman, for hosting this important hearing today. It's one of the most pressing issues facing our Nation.

Thank you to the witnesses for not only appearing today and sharing your expertise, but for taking such a leading role in protecting the integrity and security of our elections at all levels of government. It's much appreciated.

Our Nation came under attack in 2016. The special counsel described Russia's efforts to interfere in our elections as, quote, sweeping and systemic, unquote. They deceived Americans, hacked into campaign email accounts, hacked into the very systems and databases that conduct our elections at the State level.

We know that these same kinds of attacks continue to this very day. The Federal Bureau of Investigation Director Christopher Wray, stated that, quote, "this is not just an election-cycle threat.

It's pretty much a 365-day-a-year threat," unquote. Despite that, this White House has done nothing. It joins the Senate in sitting on its hands in the fight to defend our democracy. It's a real travesty, and I hope with this hearing and the legislative efforts, we can begin to turn the tide.

Unfortunately, my home State of Arizona, its voter registration database was one of Russia's targets. Their attack wasn't successful, but it shows the heightened importance local officials must place on election security.

Ms. Plunkett, you mentioned in your written testimony the importance of the integrity of voter registration databases and ePollbooks. When it comes to the use of ePollbooks for voter registration rosters and ballot-on-demand printers, do you agree that it is a best practice to use encrypted communications in all circumstances when data is transmitted or received?

Ms. PLUNKETT. Yes, I do.

Mr. STANTON. Can you think of a circumstance—is there ever a circumstance where election officials should transmit or receive data on these devices in a nonencrypted manner?

Ms. PLUNKETT. I cannot envision a circumstance such as that.

Mr. STANTON. Thank you.

Ms. Plunkett, you also mentioned that the steps the Federal Government and State governments must take will cost more than $2 billion. Not all States are adequately investing in election security. Some, including Arizona, are cutting election security funds.

What type of outcomes and risks are States that don't take this issue seriously exposing themselves to?

Ms. PLUNKETT. Well, they're exposing themselves to the potential for their election outcomes to be corrupted, invalid, not accepted, not trusted by the populous that they represent, and ultimately, the impact of the perception could be much worse than the reality, which would mean people would not come out to vote.

Mr. STANTON. Thank you for that answer.

This is a question for all of the witnesses. Some elected officials use USB devices to transfer data from one device to another. Is it best practice to use those devices only a single time to minimize the possibility of malware or to use those devices repeatedly?

Ms. BOOCKVAR. I would go with, yes, that it is certainly a best practice. There are some circumstances where as long as there's effective reformatting, that that might be effective, but I think using new ones is always, I would say, the best practice.

Mr. STANTON. Mr. Burt?

Mr. BURT. I would caution that USB devices are a known vector for the transmission of malware which can be installed at the time of their manufacture. So even using new USB devices from anything other than a very highly trusted source, and increasingly that would mean of American manufacture, if you are using it in an election in the United States, is a challenging thing to do.

You can try to scan that device, you can try to make sure it doesn't have malware on it before it's ever used, but that could be a very costly and time-consuming practice. So, the use of USB devices is something that we would say you should be very cautious about doing it even once because the malware may be present on that device when you first use it.

Mr. STANTON. Thank you.

Ms. Plunkett, have any thoughts on that subject matter?

Ms. PLUNKETT. I would go so far as to say that, unless there are no other alternatives, the use of thumb drives should be prohibited.

Mr. STANTON. Thank you very much.

I yield back.

Chairman NADLER. The gentleman yields back.

The gentlelady from Pennsylvania.

Ms. DEAN. Thank you, Mr. Chairman. Thank you for holding this important hearing.

I want to associate myself, so as not to be repetitious, with Representative Stanton's remarks of the gravity of the situation, as well as Chairman.

Secretary Boockvar, as you said—and you're not alone in saying this—nothing is more important than the security of our elections. Nothing in this democracy is more important than that. So, I am glad we're talking about these issues.

Secretary Boockvar, of course, I am delighted to see you here from Pennsylvania. I thank you and Governor Wolf for your service, particularly in the area of election security.

I'm thinking back to Mueller coming in and telling us and telling the world that certainly we—our elections were interfered with in 2016, and if I recall him correctly, he said, and it's going on 24/7. That interference continues.

Can you describe some of our vulnerabilities as of 2016 and maybe lay out some of the vulnerabilities that you still see?

Ms. BOOCKVAR. So, I think the good news—and going back to what we talked about earlier, is the good that arose from what happened in the past is that we are—with the declaration of being critical infrastructure, it's provided us with a lot more resources. So, one of the things that I really think is critically important across the country as well as in the State are these collaborations that we've been talking about. So, I think the lack of collaboration and intersection of resources could be a vulnerability if it's ignored.

So, for example, we found in Pennsylvania, as we started to have like tabletop exercises and really improve our collaborations, a lot of times in the counties, the election officials didn't even know the emergency management personnel. That's crazy, right. So, in 2018, the primary was almost like a real-life tabletop exercise. I don't know if you recall, but there was a tornado that crossed the State literally on primary day. So, we had to have—trees were down, polling places were blocked, electricity went out. The intersection of the emergency management, law enforcement, and elections was critical—is critical.

So, one of the vulnerabilities is not feeding that well. Again, it goes back to the COOP planning, too. Then I also want to make sure that our counties have the resources they need to have really advanced intrusion detection systems, effective plan—training of phishing and security and all that, and every advanced sensor and protection, layered defenses of their network.

So, those are the areas that I would really focus on. Supporting the local counties and municipalities would be one of the areas I'd want to direct most attention.

Ms. DEAN. The issue of certification, I guess, of the equipment itself, what is the delay there? How could we streamline that? Either you or any of the witnesses.

Mr. BURT. The issue there is that the standards that—the guidelines that are promulgated by the Election Assistance Commission are more than 10 years old. In fact, the most recent modification of those guidelines, there's not a single election system that's ever been certified under those most recent guidelines, and they're 10 years old.

So, what the Election Assistance Commission is doing right now, which is revising those guidelines, is critically important, but they need to move quickly. They need to move with expeditious activity, because this threat, as you pointed out, Congresswoman, is 24/7. It's happening now. It's going to happen through the 2020 election cycle.

So, we need the EAC to adopt new guidelines for certification quickly. The current ones are—don't adequately address security, and they take too long and they're too burdensome. So, we need to streamline that process, make it faster.

One of the really critical things for all State and local election officials is we need to make it very easy to apply security updates. That's a key defense to these adversaries from every vendor, and so we need to be able to apply security updates quickly, expeditiously, without so much bureaucracy so that we can respond.

Ms. DEAN. Thank you very much.

This will just be by way of sort of a rhetorical statement. I was struck by something you wrote in your testimony, Secretary Boockvar. You wrote that election security is a race without a finish line, that our adversaries are continuously advancing their technologies, and we must do more all the time. So, we know that we can't see a finish line for this, and we have to identify the threats.

I have to wonder what conversations all of you have had to have with your own organizations based on foreign threats, but now the news of this past week, domestic threat to our election. It couldn't be a more grievous, grave time. None of us is pleased with the news of the Ukraine conversation by the President of the United States in an attempt to interfere in a future election. So, I praise you all for your work. Help us do better at our work to protect our elections.

I yield back.

Chairman NADLER. The gentlelady yields back.

This concludes today's hearing. We thank all our witnesses for participating.

Without objection, all Members will have 5 legislative days to submit additional written questions for the witnesses or additional materials for the record.

With that, without objection, the hearing is adjourned.

[Whereupon, at 12:02 p.m., the Committee was adjourned.]

APPENDIX

BRENNAN CENTER FOR JUSTICE

House Committee on the Judiciary
United States House of Representatives

Statement for the Record
Brennan Center for Justice at NYU School of Law

"Securing America's Elections"

September 27, 2019

The Brennan Center thanks the House Committee on the Judiciary for holding this hearing on the critical issue of election security. The Brennan Center for Justice—a nonpartisan law and policy institute that focuses on democracy and justice—appreciates the opportunity to provide detailed information about election infrastructure vulnerabilities and important remedial policies and procedures we have identified in our extensive studies and efforts to ensure our nation's election systems are more secure and reliable in today's complex threat environment. We are deeply involved in the effort to ensure accurate and fair voting for all Americans.

Our country has made significant progress to secure our election infrastructure from cyber-attack since 2016.[1] Federal, state and local officials continue to implement fundamental systemic and infrastructure improvements.[2] Yet, significant security gaps

[1] Lawrence Norden and Andrea Cordova, "Voting Machine Security: Where We Stand Six Months Before the New Hampshire Primary," *Brennan Center for Justice*, August 13, 2019, https://www.brennancenter.org/analysis/voting-machine-security-where-we-stand-six-months-new-hampshire-primary.

[2] Ibid; Election Security Hearing, Before the Comm. on House Administration, 116th Cong. (2019) (statement of Lawrence Norden) ("The designation by the Department of Homeland Security ("DHS") of election infrastructure as critical infrastructure means state and local election offices have priority access to needed resources, including cybersecurity advisors and risk assessments. As a result, election officials have participated in thousands of hours of cybersecurity trainings and table-top exercises to prevent, detect, and recover from intrusions into critical election infrastructure. DHS and the Election Assistance Commission ("EAC") have facilitated much better information sharing between election system vendors, the states, and the federal government. Finally, in 2018 Congress provided $380 million in Help America Vote Act ("HAVA") funds to help states bolster their election security. Finally, in 2018 Congress provided $380 million in Help America Vote Act ("HAVA") funds to help states bolster their election security. Based on information provided by the EAC, we know that roughly 85% of this money will be spent prior to the presidential election on such critical measures as strengthening election cybersecurity, purchasing new

remain, many on a patchwork basis across the country.[3] This landscape is largely the result of our decentralized electoral system. While this structure is a strength in many ways, as a nation, we are only as strong as our weakest link. Successful attacks against our infrastructure in any county in any state can have a ripple effect that impacts the balance of power at the federal level and the daily lives of American citizens.

Additional, and urgent, action is required to ensure that our country's election infrastructure is sufficiently resilient to withstand future attacks. In the testimony below, we identify five risks to our election infrastructure, as well as steps that can be taken to reduce their potential harm: (1) the continued use of paperless and antiquated voting systems; (2) the lack of a federal certification program for electronic pollbooks; (3) the rapid evolution of cyber threats; (4) the lack of federal oversight of election system vendors; (5) the limited resources of state and local election officials.

Too Many Jurisdictions Still Use Paperless and Antiquated Voting Systems. We Must Replace Them and Implement Robust Post-Election Audits.

Millions of voters will go to the polls to cast their ballot on Election Day 2020. They will encounter a variety of different voting machines at their polling place and we estimate at least some voters in as many as 38 states will cast their ballot on equipment that is more than 10 years old.[4] In November 2018, we estimate that 34 percent of all local election jurisdictions were using voting machines that were at least 10 years old as their primary polling place equipment (or as their primary tabulation equipment in all vote-by-mail jurisdictions)[5] and 20 years old in at least one state.[6]

These aging voting systems are a security risk and less reliable than voting equipment available today. Older systems are generally "more likely to fail and are increasingly

---

voting equipment, and improving post election audits, all essential steps in protecting our elections from foreign interference.")

[3] DHS National Risk Management Center, July 2018, https://www.dhs.gov/sites/default/files/publications/18_0731_cyber-summit-national-risk-management-fact-sheet.pdf.

[4] Lawrence Norden and Andrea Cordova, "Voting Machine Security: Where We Stand Six Months Before the New Hampshire Primary," *Brennan Center for Justice*, August 13, 2019, https://www.brennancenter.org/analysis/voting-machine-security-where-we-stand-six-months-new-hampshire-primary (41 states minus Alaska, California, and North Dakota).

[5] Ibid.

[6] "Proposed Recommendation Regarding Acquisition of a New Voting System," Alaska Election Policy Work Group, http://www.elections.alaska.gov/doc/info/180718%20DRAFT%20Proposition.pdf.

difficult to maintain."[7] Many are no longer manufactured so finding replacement parts will be increasingly difficult over time.[8] This problem exacerbates the reported system-specific security concerns with some widely used older systems, such as the AutoMARK, including inconsistent vote tallying and reboot times of 15 to 20 minutes.[9] Moreover, these systems simply lack important security features expected of voting machines today, such as hardware access deterrents for ports.[10]

More troubling, we estimate that, absent additional federal assistance, at least some voters in 8 states (Indiana, Kansas, Kentucky, Louisiana, Mississippi, New Jersey, Tennessee and Texas) will cast their ballots on paperless voting systems in 2020.[11] Voter-marked paper ballots are a critical election security measure[12] and, in the event a virus or other malicious software is introduced into a voting machine, can be used to detect and recover from that attack.

Paper-based systems also provide better security because they create a paper record that voters can review before casting their ballot and election officials can audit after the

---

[7] *Election Security Hearing*, *Before the Comm. on House Administration*, 116th Cong. (2019) (statement of Lawrence Norden); Josie Bahnke (Elections Director, Office of the Lieutenant Governor, Alaska), Letter to Election Policy Work Group Members, July 18, 2018, http://www.elections.alaska.gov/doc/info/180718%20EPWG%20Research.pdf ("Today the DOE is at a critical juncture: Alaska's voting equipment and technology are outdated, difficult to repair and prone to failure").

[8] Lawrence Norden and Andrea Cordova, "Voting Machines at Risk: Where We Stand Today," *Brennan Center for Justice*, March 5, 2019, https://www.brennancenter.org/analysis/voting-machines-risk-where-we-stand-today.

[9] Ruth Johnson (Oakland County clerk/register of deeds), Letter to Rosemary Rodriguez (chairperson, Election Assistance Commission), October 2, 2008, https://www.eac.gov/assets/1/6/Oakland_County_Michigan_letter_regarding_ES_S_M-100_voting_machine_tabulators.pdf (stating that 8 percent of M-100 fleet in Oakland County "reported inconsistent vote totals during their logic and accuracy testing"); "Election Systems and Software (ES&S) AutoMARK," Verified Voting (listing AutoMARK security concerns), accessed May 4, 2019, https://www.verifiedvoting.org/resources/voting-equipment/%20ess/automark/.

[10] Christopher R. Deluzio, Liz Howard, Paul Rosenzweig, David Salvo, Rachael Dean Wilson, *Defending Elections*, Brennan Center for Justice, 2019, https://www.brennancenter.org/sites/default/files/publications/2019_07_EACFunding%20Report_FINAL.pdf.

[11] Lawrence Norden and Andrea Cordova, "Voting Machine Security: Where We Stand Six Months Before the New Hampshire Primary," *Brennan Center for Justice*, August 13, 2019, https://www.brennancenter.org/analysis/voting-machine-security-where-we-stand-six-months-new-hampshire-primary.

[12] *Securing the Vote*, The National Academies of Sciences, Engineering, and Medicine, 2018, https://www.nap.edu/read/25120/chapter/1; *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations*, U.S. Senate Select Committee on Intelligence, May 8, 2018, https://www.intelligence.senate.gov/publications/russia-inquiry.

election. However, these paper records will be of little security value unless they are used to check and confirm electronic tallies of election results. In 2020, we estimate that only 24 states and the District of Columbia will have voter verifiable paper records for all votes cast and require post-election audits of those paper records before certifying election results.[13]

The Brennan Center has long supported both a complete, nationwide transition to paper ballot voting machines and the implementation of risk limiting audits ("RLAs"), an efficient and effective check on election results, to ensure security and confidence in electoral results.

Encouragingly, multiple states have made significant progress in replacing their aging and paperless systems in recent years. Arkansas, Georgia, Pennsylvania and South Carolina have either completed the replacement of their paperless voting machines or are transitioning now.[14] Alaska, California, North Dakota and Ohio are currently working to replace their aging systems.[15] In addition, at least 12 states are experimenting with risk-limiting audits, the "gold-standard" of post-election audits.

There Are No Federal Security Guidelines for Electronic Pollbooks. They Should Be Included in the Federal Certification Process.

As of July 2019, 41 states and DC use or authorize the use of electronic pollbooks in at least some polling places.[16] Electronic pollbooks (EPBs) are laptops or tablets that poll workers use instead of paper lists to look up voters. Most EPBs can communicate with other EPBs in the same polling location to share real-time voter check-in updates.[17] In addition to an expedited check-in procedure, shorter lines, lower staffing needs, and cost savings, one major benefit of EPBs is that they can make it easier to set up "vote centers" during early voting or on Election Day. Vote centers are "an alternative to traditional

---

[13] Lawrence Norden and Andrea Cordova, "Voting Machine Security: Where We Stand Six Months Before the New Hampshire Primary," *Brennan Center for Justice*, August 13, 2019, https://www.brennancenter.org/analysis/voting-machine-security-where-we-stand-six-months-new-hampshire-primary.

[14] Ibid.

[15] Ibid.

[16] "Electronic Poll Books," National Conference of State Legislatures, July 15, 2019, http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx; Andrea Cordova, "Want a Simple Way to Increase Election Security? Use Paper," *Brennan Center for Justice*, October 8, 2018, https://www.brennancenter.org/blog/want-simple-way-increase-election-security-use-paper.

[17] Edgardo Cortés, Liz Howard, and Lawrence Norden, *Better Safe than Sorry: How Election Officials can Plan Ahead to Protect the Vote in the Face of a Cyberattack*, Brennan Center for Justice, 2018, https://www.brennancenter.org/sites/default/files/publications/2018_08_13_ElectionSecurity_V4.pdf.

neighborhood-based precincts."[18] Anyone in a particular jurisdiction can vote there, regardless of where they live, possibly making voting more convenient, providing additional cost savings, and encouraging increased voter turnout.[19] If a county uses multiple vote centers, the electronic pollbooks can automatically sync during the day to ensure that once someone has voted in a particular location, they cannot vote in another location on the same day.

Despite these advantages, EPBs also pose significant risks. In a worst-case scenario, hackers could alter or delete voter data, even causing voters to appear as if they have voted when they have not. EPBs that require access to the Internet can also pose problems in rural counties that lack reliable connectivity.[20] Unlike voting machines, there are currently no national security standards for electronic pollbooks. HAVA's current structure limits EAC's ability to create requirements for, test, and certify EPBs in the same way they do for voting machines.

In the absence of federal certification standards, states have developed a patchwork system of e-pollbook regulation and certification. Only 12 states certify systems statewide, according to NCSL.[21] Many states using EPBs do not mandate important election security measures that can mitigate risks associated with EPB use in precincts. In 2018, when 34 states used EPBs, only half required printed backup paper pollbooks to be present in the polling place at the time voting began and, in 32 of the 34 states, we found no requirements in state law or regulation mandating a minimum number of provisional ballots.[22]

The Brennan Center supports updating the Help American Vote Act to allow the EAC to create a certification program for all electronic pollbooks, as they do for voting systems, in order to encourage secure EPB systems nationwide. These additional responsibilities will require increased funding and staffing levels for the EAC to effectively test and certify EPBs.

---

[18] "Vote Centers," National Conference of State Legislatures, http://www.ncsl.org/research/elections-and-campaigns/vote-centers.aspx.
[19] Ibid.
[20] Andrea Cordova, "Want a Simple Way to Increase Election Security? Use Paper," *Brennan Center for Justice*, October 8, 2018, https://www.brennancenter.org/blog/want-simple-way-increase-election-security-use-paper.
[21] "Electronic Poll Books," National Conference of State Legislatures, July 15, 2019, http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx.
[22] Andrea Cordova, "Want a Simple Way to Increase Election Security? Use Paper," *Brennan Center for Justice*, October 8, 2018, https://www.brennancenter.org/blog/want-simple-way-increase-election-security-use-paper.

Cyberthreats Evolve and Change Over Time. It Is Critical to Conduct Penetration Testing and Nationwide Threat Assessments to Keep Up.

In addition to including EPBs in the testing and certification process, the Brennan Center recommends creating an additional requirement of penetration testing for each EAC-vetted system. Penetration testing proactively identifies vulnerabilities in critical infrastructure, often by launching real-world attacks on the system. Once vulnerabilities are discovered, they can be cured before malicious actors become aware of them.[23]

Penetration testing is a critical addition due to the limitations of the current federal certification process, which only ensures compliance with baseline security requirements created using information available before the time of certification. Unlike the static certification process, penetration testing protocols can be updated on an ongoing basis in response to the ever-evolving threat environment. Periodic penetration testing of both new and existing EAC-vetted election systems should be made a routine part of the EAC certification process. This process could leverage the skills and expertise of technology companies and white hat hackers to find potential system vulnerabilities. This would ensure that our election systems are prepared to meet the challenge of defending against a landscape of new and changing cyber threats.

The Brennan Center also supports a requirement that the federal government conduct regular, nationwide threat assessments to help state and local governments understand where the vulnerabilities to cyberattack are. As cyber threats evolve, it is critical to conduct ongoing threat assessments of election infrastructure such as voter registration databases and voting systems. Conducting threat assessments on a regular basis would help state and local governments implement mitigation strategies where weaknesses are identified. In a 2017 Brennan Center report, *Securing Elections from Foreign Interference*, we noted a consensus among experts that many states were unlikely to have completed this kind of risk assessment in the last few years, even though the cost of completing a threat assessment was likely to be manageable. In the Commonwealth of Virginia, for example, Edgardo Cortés, former Commissioner of the Virginia Department of Elections and current Brennan Center Election Security Advisor, estimates that his department

[23] Meredith Berger, Charles Chretien, Caitlin Conley, Jordan D'Amato, Meredith Davis Tavera, Corinna Fehst, Josh Feinblum, Kunal Kothari, Alexander Krey, Richard Kuzma, Ryan Macias, Katherine Mansted, Henry Miller, Jennifer Nam, Zara Perumal, Jonathan Pevarnek, Anu Saha, Mike Specter and Sarah Starr, *The State and Local Election Cybersecurity Playbook*, Harvard Kennedy School and Defending Digital Democracy, 2018, 53, https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf.

could have conducted a comprehensive threat assessment or audit for just $80,000 annually.[24]

Election System Vendors Are Another Point of Vulnerability. They Should be Required to Report Cybersecurity Incidents.

Private companies are contracted to perform everything from building and maintaining election websites that help voters determine how to register and where they can vote, to printing and designing ballots, to programming voting machines before each election, to building and maintaining voter registration databases, voting machines, and electronic poll books. Congress should consider additional steps to protect our elections from attacks that target these private election system vendors and to regulate vendor conduct. Unlike other sectors that the federal government has designated "critical infrastructure," there is currently almost no federal oversight of the private vendors who design, build and maintain our election systems. In fact, there are more federal regulations for ballpoint pens and magic markers than there are for voting systems and other parts of our federal elections infrastructure.

The Brennan Center recommends that Congress adopt a mandatory reporting system for all cyber security incidents for election vendors. While this may seem like a small step, it will have a large impact on the overall security position of election officials around the country. Election vendors have stated that such requirements are unnecessary and burdensome, and that they are somehow different from vendors in other critical infrastructure sectors. This is simply not true. We know that the lack of transparency in vendor security is a significant vulnerability to election security. Private vendors were targeted in the 2016 election and are likely to be targeted again.[25] In fact, reporting requirements for cyber security incidents are a bare minimum, and we should be considering additional requirements such as vendor employee background checks and other lessons learned from similar critical infrastructure sectors.[26] The Brennan Center

[24] Lawrence Norden and Ian Vandewalker, *Securing Elections from Foreign Interference*, Brennan Center for Justice, 2017, https://www.brennancenter.org/publication/securing-elections-foreign-interference.
[25] Lawrence Norden and Ian Vandewalker, *Securing Elections from Foreign Interference*, Brennan Center for Justice, 2017, https://www.brennancenter.org/publication/securing-elections-foreign-interference.
[26] Brian Calkin, Kelvin Coleman, Brian de Vallance, Thomas Duffy, Curtis Dukes, Mike Garcia, John Gilligan, Paul Harrington, Caroline Hymel, Philippe Langlois, Adam Montville, Tony Sager, Ben Spear, Roisin, *A Handbook for Elections Infrastructure Security*, Center for Internet Security, February 2018, https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf.

has documented some of the additional reasons for mandating such reporting in the 2010 report, *Voting System Failures: A Database Solution*.[27]

Election Officials Have Limited Resources. Congress Should Ensure That They Have Sufficient Funding to Protect Our Election Infrastructure.

Congress took an important first step in 2018 by allocating $380 million to states for election security activities. However, it is clear there is an ongoing need for federal funding to help protect our elections infrastructure from foreign threats. Congress should build on last year's efforts and provide additional funding to states to continue improving election security. Any funding should ensure that some of it is designated for use at the local level. In addition to funding for state and local election offices, Congress should ensure that federal agencies involved in this important work, including EAC, DHS, and NIST, have sufficient resources to carry out their mandates.

Conclusion

With significant risks threatening our election infrastructure, effective risk mitigation measures and policies should be uniformly implemented to create a resilient election administration system. We are encouraged by the great progress we have made in securing our elections since 2016, but our work in defending against cyber threats is far from complete. Election officials around the country need appropriate tools and resources to meet the on-going challenge of protecting our democracy from hostile nation states. We urge you to consider legislative changes that will help tackle these problems head on. We appreciate this committee's leadership in continuing to strengthen our nation's election infrastructure.

[27] Lawrence Norden, *Voting System Failures: A Database Solution*, Brennan Center for Justice, 2010, https://www.brennancenter.org/publication/voting-system-failures-database-solution.