SECURE, SAFE, AND AUDITABLE: PROTECTING THE INTEGRITY OF THE 2020 ELECTIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

AUGUST 4, 2020

Serial No. 116–81

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

43–954 PDF WASHINGTON : 2021

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
CEDRIC L. RICHMOND, Louisiana
DONALD M. PAYNE, JR., New Jersey
KATHLEEN M. RICE, New York
J. LUIS CORREA, California
XOCHITL TORRES SMALL, New Mexico
MAX ROSE, New York
LAUREN UNDERWOOD, Illinois
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
NANETTE DIAZ BARRAGÁN, California
VAL BUTLER DEMINGS, Florida
MIKE ROGERS, Alabama
PETER T. KING, New York
MICHAEL T. MCCAUL, Texas
JOHN KATKO, New York
MARK WALKER, North Carolina
CLAY HIGGINS, Louisiana
DEBBIE LESKO, Arizona
MARK GREEN, Tennessee
JOHN JOYCE, Pennsylvania
DAN CRENSHAW, Texas
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
JEFFERSON VAN DREW, Texas
MIKE GARCIA, California

HOPE GOINS, *Staff Director*
CHRIS VIESON, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

CEDRIC L. RICHMOND, Louisiana, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
KATHLEEN M. RICE, New York
LAUREN UNDERWOOD, Illinois
ELISSA SLOTKIN, Michigan
BENNIE G. THOMPSON, Mississippi *(ex officio)*
JOHN KATKO, New York, *Ranking Member*
MARK WALKER, North Carolina
MARK GREEN, Tennessee
JOHN JOYCE, Pennsylvania
MIKE ROGERS, Alabama *(ex officio)*

MOIRA BERGIN, *Subcommittee Staff Director*
SARAH MOXLEY, *Minority Subcommittee Staff Director*

CONTENTS

SECURE, SAFE, AND AUDITABLE: PROTECTING THE INTEGRITY OF THE 2020 ELECTIONS

Tuesday, August 4, 2020

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY,
INFRASTRUCTURE PROTECTION,
AND INNOVATION,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:02 a.m., via Webex, Hon. Cedric L. Richmond (Chairman of the subcommittee) presiding.

Present: Representatives Richmond, Jackson Lee, Langevin, Rice, Underwood, Slotkin, Thompson (ex officio), Katko, and Joyce.

Also present: Representatives Demings, and Green of Texas.

Mr. RICHMOND. The Subcommittee on Cybersecurity, Infrastructure, Protection, and Innovation will come to order.

Good morning. I want to thank the witnesses for participating in today's hearing. We all have a stake in ensuring a safe, secure election in November. This hearing comes a week after we laid to rest a giant in the right for voting rights—in the fight for voting rights. Before he died, Congressman Lewis reminding us that the vote is the most powerful, nonviolent change agent you have in a Democratic society. You must use it because it is not guaranteed. You can lose it. We must vigorously defend our right to vote, our access to the ballot box, and the integrity of our election.

In less than 90 days, Americans across the country will participate in an election unlike any other in our history. The COVID–19 pandemic is forcing State and local election officials to rapidly expand vote-by-mail, early voting, and other crowd-reducing election policies so no voter has to choose between their democratic rights and their health.

As States scramble to administer safe primary elections this spring, seemingly, administrative decisions related to the number and location of polling sites had substantive impacts on people's right to vote. Long lines and crowded polling locations in predominantly Black and Brown neighborhoods raise the stress levels in communities disproportionately impacted by COVID–19. Police violence that underscored that existence of systematic racism as an injustice that we must still overcome.

We have a President who has repeatedly tried to manipulate a news cycle, going so far as to falsely suggest he can move the elec-

tion date, and, more insidiously, making baseless claims about the security of vote-by-mail. This behavior is in service to his own narcissistic political ends, softens the turf for dangerous foreign influence campaigns, and puts Americans who want to exercise the franchise at risk.

For the record, the President does not have the power to move the date of the election from November. Moreover, last Friday, the Cybersecurity Infrastructure Security Agency released a risk assessment of vote-by-mail. CISA concluded that while there are risks associated with mail-in voting, just as with every other method of voting, those risks can be mitigated.

Further, I am not a voyeur of any intelligence assessment indicating that foreign actors have expressed interest or capability to successfully interfere with vote-by-mail processes. We must learn the lessons of our recent elections and do better in November.

First, we must prepare Americans for the reality that elections will be administered differently this fall. We must educate voters about vote-by-mail, its related deadlines, and how expanded vote-by-mail might affect the timing of election results. We must encourage participation in vote-by-mail while inoculating the public from disinformation campaigns aimed at undermining confidence in election results.

Second, we must ensure that changes to the USPS service standards do not jeopardize vote-by-mail, and that the election officials seeking to expand vote-by-mail coordinate with the Postal Service to coordinate vote-by-mail policies and deadlines.

Third, we must ensure election officials do not use COVID–19 as a pretext for making administrative decisions that could disenfranchise voters.

Time and time again, the impacts of dysfunctional and chaotic election administration falls hardest on Black and Brown communities. Election officials must be deliberate in their efforts to ensure that no community is disenfranchised.

Fourth, we must not forget the lessons of 2016. It was around this time in 2016 when a Russian foreign interference campaign engaged in hack-and-dump-operations against one candidate, and targeted election systems in all 50 States.

We must continue to improve the election—the security of election infrastructure and campaign organizations, and improve the public resilience to foreign influence campaigns.

Finally, we need to be honest with ourselves about what it will take to administer safe, secure, and auditable elections this fall. It has been over 10 weeks since the House passed the HEROES Act, which would have provided $3.6 billion in funding to support State and local election officials. Despite urgent requests for additional resources from State and local election officials across the country, the Senate never voted on the HEROES Act, nor did it include any election administration funding in the COVID response package it released last week.

As the House and Senate negotiations on COVID relief package continues, I urge my Senate colleagues to step up and provide State and local election officials the funding they need to administer safe, secure, and auditable elections this November.

I look forward to hearing from the witnesses today, their recommendations for Congress on ways to give Americans more opportunities to vote this November, and to ensure the safety and integrity of the election.

[The statement of Chairman Richmond follows:]

STATEMENT OF CHAIRMAN CEDRIC L. RICHMOND

AUGUST 4, 2020

We all have a stake in ensuring safe, secure, and auditable elections in November. This hearing comes a week after we laid to rest a giant in the fight for voting rights. Before he died, Congressman Lewis reminded us that "[t]he vote is the most powerful nonviolent change agent you have in a democratic society. You must use it because it is not guaranteed. You can lose it." We must vigorously defend our right to vote, our access to the ballot box, and the integrity of our elections.

In less than 100 days, Americans across the country will participate in an election unlike any other in our history. The COVID–19 pandemic is forcing State and local election officials to rapidly expand vote-by-mail, early voting, and other crowd-reducing election policies so no voter has to choose between their democratic rights and their health.

As States scrambled to administer safe primary elections this spring, seemingly administrative decisions related to the number and location of polling sites had substantive impacts on people's voting rights. Long lines and crowded polling locations in predominantly black and brown neighborhoods raised the stress levels in communities disproportionately impacted by COVID–19 and police violence and underscored that the existence of systemic racism as is an injustice that we must still overcome. We have a President who has repeatedly tried to manipulate a news cycle, going so far as to falsely suggest he can move the election date and, more insidiously, making baseless claims about the security of vote-by-mail.

This behavior, in service to his own narcissistic political ends, softens the turf for dangerous foreign influence campaigns and puts Americans who want to exercise the franchise at risk. For the record, the President does not have the power to move the date of the November election. Moreover, last Friday the Cybersecurity and Infrastructure Security Agency released a risk assessment of vote-by-mail.

CISA concluded that while there are risks associated with mail-in voting—just as there with every other method of voting—those risks can be mitigated. Further, I am not aware of any intelligence assessment indicating that foreign actors have expressed interest or capability to successfully interfere with vote-by-mail processes. We must learn the lessons of our recent elections and do better in November.

First, we must prepare Americans for the reality that elections will be administered differently this fall. We must educate voters about vote-by-mail, its related deadlines, and how expanded vote-by-mail might affect the timing of election results. We must encourage participation in vote-by-mail while inoculating the public from disinformation campaigns aimed at undermining confidence election results.

Second, we must ensure that changes to USPS service standards do not jeopardize vote-by-mail, and that election officials seeking to expand vote-by-mail coordinate with the Postal Service to coordinate vote-by-mail policies and deadlines. Third, we must ensure election officials do not use COVID–19 as a pretext for making administrative decisions that could disenfranchise voters. Time and again, the impacts of dysfunctional and chaotic election administration fall hardest on black and brown communities. Election officials must be deliberate in their efforts to ensure that no community is disenfranchised.

Fourth, we must not forget the lessons of 2016. It was around this time in 2016 when the Russian foreign interference campaign engaged in hack-and-dump operations against one candidate, and targeted election systems in all 50 States. We must continue to improve the security of election infrastructure and campaign organizations, and improve the public's resilience to foreign influence campaigns.

Finally, we need to be honest with ourselves about what it will take to administer safe, secure, and auditable elections this fall. It has been over 10 weeks since the House passed the HEROES Act, which would provide $3.6 billion in funding to support State and local election officials. Despite urgent requests for additional resources from State and local election officials across the country, the Senate never voted on the HEROES Act, nor did include any election administration funding in the COVID response package it released late last month.

As House and Senate negotiations on COVID relief package continue, I urge my Senate colleagues to step up and provide State and local election officials the fund-

ing they need to administer safe, secure, and auditable elections this November. I look forward to hearing from the witness today their recommendations for Congress on ways to give Americans more opportunities to vote this November, and to ensure the safety and integrity of the election.

Mr. RICHMOND. I ask unanimous consent that Mrs. Demings of Florida and Mr. Green of Texas be permitted to participate in today's hearing without objection.

With that, I would like to recognize the Ranking Member of the subcommittee, Mr. Katko of New York, for any opening statements he may have.

Mr. KATKO. Thank you, Mr. Chairman. I want to echo your sentiment at the outset about John Lewis. He truly was a giant in American politics and American leadership, and I considered him a friend, and his legacy will live on long after his passing, that is for sure.

I want to thank the CAT staff for accommodating the schedule today. I have another example of how bad 2020 is. My best friend's son is being laid to rest this morning, and so it is, it is another awful—another awful example of this awful year.

I want to thank Chairman Richmond for holding this important hearing. Election security is something that I am very concerned about. I have been working hard to ensure that all Americans are able to vote securely and have their vote counted.

Although we have made significant progress since 2016, elections security remains a major concern of mine. Secure voting systems and accurate reporting of votes are fundamental to our democracy. Americans should have full confidence in every aspect of our election process.

I want to applaud the elections security efforts by the Cybersecurity and Infrastructure Agency that are known as CISA, and its partnerships with State, local, territorial, and Tribal governments that have resulted in a marked improvement of election security over 2016. CISA provides State and local officials the technical assistance, playbooks, and exercises, shares information on threats, and assists us responding to cyber incidents.

The pandemic has injected new elements of uncertainty into the 2020 election that have forced many local election officials to reinvent the process by which citizens vote. These changes will keep citizens and poll workers safe while maintaining citizens' faith in the process.

In March, Congress provided $400 million in the new Help America Vote Act or HAVA funds to States to prepare for and conduct a 2020 election during the pandemic. Aided by this infusion of funding, State and local election officials are adjusting to huge increases in voting-by-mail and the consolidation of voting locations.

CISA is also working with State and local election officials to head off disinformation campaigns engineered by adversaries. A key component of this strategy is countering the opportunity for adversaries to spread disinformation on remote-voting procedures and changes in polling locations.

CISA has assisted State and local officials with methods to drive voters to reliable sources of information, and how to communicate changes to election procedures, polling locations, and times.

Election security for 2020 has also improved as a result of the growing participation in the Election Infrastructure ISAC by State and local officials. The Election ISAC has provided thousands of election offices with the cyber resources they need to maintain the reliability of their election infrastructure, including best practices, tools, training, and perhaps, most important, information sharing and analysis.

However, many election offices don't have the IT knowledge or resources necessary to take advantage of this information. Some of them feel deluged with information that they simply cannot sift through or handle from the ISAC. These local election offices are not equipped to handle the cyber threats to the election infrastructure alone. This is why I introduced my Cyber Navigators Bill, which authorizes grants for State and local governments to hire cybersecurity experts to provide risk management, resiliency, and technical support in the administration of elections. My bill enables the State to hire a cybersecurity expert familiar with the State's unique election systems. The regional nature of the assistance ensures that those navigators are able to establish relationships with their regional and State election officials. By targeting this assistance at the administration of elections, State election officials aren't forced to compete with other State priorities. Election security has a history of bipartisan cooperation and support. Ensuring that our election process is uncompromised during the upcoming election must remain a top priority from both sides of the aisle.

Together, I look forward to continuing to work toward the goal with my colleagues on the subcommittee. I thank the witnesses for providing the subcommittee with their testimony, and I look forward to hearing their ideas in how we can further improve the security of our election systems. With that, Mr. Chairman, I yield back.

[The statement of Ranking Member Katko follows:]

STATEMENT OF RANKING MEMBER JOHN KATKO

AUGUST 4, 2020

Thank you, Mr. Chairman.

I want thank Chairman Richmond for holding this important hearing.

Although we have made significant progress since 2016, election security remains a major concern of mine. Secure voting systems and the accurate reporting of votes are foundational to our democracy. Americans should have full confidence in every aspect of our election process.

I want to applaud election security efforts led by Cybersecurity and Infrastructure Security Agency (CISA) and its partnerships with State, local, territorial, and Tribal governments that have resulted in a marked improvement of election security over 2016. CISA provides State and local officials with technical assistance, playbooks, and exercises, shares information on threats, and assists with responding to cyber incidents.

The pandemic has injected new elements of uncertainty into the 2020 elections that have forced many local election officials to reinvent the process by which citizens vote. These changes will keep citizens and poll workers safe while maintaining citizens' faith in the process. In March, Congress provided $400 million in new Help American Vote Act (HAVA) funds to States to prepare for and conduct the 2020 Election during the pandemic. Aided by this infusion of funding, State and local election officials are adjusting to huge increases in voting-by-mail and the consolidation of voting locations.

CISA is also working with State and local election officials to head off disinformation campaigns engineered by adversaries. A key component of this strategy is countering the opportunity for adversaries to spread disinformation on remote

voting procedures and changes in polling locations. CISA has assisted State and local officials with methods to drive voters to reliable sources of information, and how to communicate changes to election procedures, polling locations, and times.

Election security for 2020 has also improved as a result of the growing participation in the Election Infrastructure ISAC (EI–ISAC) by State and local election officials. The EI–ISAC has provided thousands of election offices with the cyber resources they need to maintain the reliability of their election infrastructure including best practices, tools, training, and information sharing and analysis.

However, many local election offices don't have the IT knowledge or resources necessary to take advantage of this information. These local election offices are not equipped to handle cyber threats to their election infrastructure alone.

This is why I introduced my Cyber Navigators bill which authorizes grants for State and local governments to hire cybersecurity experts to provide risk management, resiliency, and technical support in the administration of elections. My bill enables a State to hire a cybersecurity expert familiar with a State's unique election systems. The regional nature of the assistance ensures that these navigators are able to establish relationships with their regional and State election officials. By targeting the assistance at the administration of elections, State election officials aren't forced to compete with other State priorities.

Election security has a history of bipartisan cooperation and support. Ensuring that our election process is uncompromised during the upcoming election must remain a top priority for both sides of the aisle. I look forward to continuing to work toward this goal with my colleagues on the subcommittee.

I thank the witnesses for providing the subcommittee with their testimony and I look forward to hearing their ideas on how we can further improve the security of our election systems.

I yield back.

Mr. RICHMOND. The gentleman from New York yields back.

Mr. Katko, we will all be saying prayers for you as you attend the funeral, and we thank you for your attendance.

Mr. KATKO. Thank you. Say a lot of prayer. I have got to deliver the eulogy, and it is going to be a tough one. So thank you, Mr. Chairman.

Mr. RICHMOND. Thank you. Members are reminded that the subcommittee will operate according to the guidelines laid out by the Chairman and Ranking Member in the July 8 colloquy. With that, I ask unanimous consent to waive Committee Rule 882 for the subcommittee during remote proceedings under the covered period designated by the Speaker under the House Resolution 965. Without objection, so ordered.

The Chair now recognizes the Chairman of the full committee, the gentleman from Mississippi, Mr. Thompson, for an opening statement.

Maybe we don't. Do we have Mr. Thompson here?

The Chair will now—we will go on to the Ranking Member of the full committee, and then we will come back to the Chairman.

So now the Chair recognizes the Ranking Member of the full committee, the gentleman from Alabama, Mr. Rogers, for an opening statement. Mr. Rogers is not here.

So let's do this, let's go straight to our amazing witnesses. So I will now welcome our panel of witnesses. First, I would like to welcome David Levine, an elections integrity fellow at the Alliance for Securing Democracy. Mr. Levine previously served in a range of positions administering and observing elections and advocating for election reform, including as the Ada County, Idaho elections director and as the director of elections for the city of Richmond, Virginia.

Next, Ms. Sylvia Albert, the director of Voting and Elections, Common Cause. Ms. Albert brings more than a decade of profes-

sional experience in public interest law, and public policy campaigns, expanding ballot access, reducing barriers to participation, and combating voter intimidation among historically disenfranchised communities.

Next, we will hear from Ms. Amber McReynolds, CEO for the National Vote at Home Institute and Coalition. She is the former director of elections for Denver, Colorado, and serves on a National election task force on election crises. As a former election official in a State with universal vote-by-mail, I look forward to hearing her unique perspective on that topic.

Finally, we have Mr. John Gilligan, the president and CEO of the Center for Internet Security, or CIS. Together with Elections Infrastructure, Information Sharing, and Analysis Center, EI–ISAC, provides many resources to support the Cybersecurity needs of the election community.

I appreciate you all joining us today. Without objection, the witnesses' full statements will be inserted for the record. I now ask each witness to summarize his or her statement for 5 minutes, beginning with Mr. Levine.

STATEMENT OF DAVID LEVINE, ELECTIONS INTEGRITY FELLOW, ALLIANCE FOR SECURING DEMOCRACY, GERMAN MARSHALL FUND OF THE UNITED STATES

Mr. LEVINE. Chairman Richmond, Ranking Member Katko, and Members of this subcommittee on Cybersecurity, Infrastructure Protection, and Innovation. Good morning, and thank you for the opportunity to testify today on protecting the integrity of the 2020 elections during the COVID–19 pandemic.

My name is David Levine, and I am the elections integrity fellow for the Alliance for Securing Democracy, a bipartisan, Transatlantic initiative housed within the German Marshall Fund of the United States. ASD develops comprehensive strategies to defer and defend against authoritarian efforts to undermine and interfere with Democratic institutions.

The 2020 primary election season has been unique with a global pandemic, Nation-wide protests, and an on-going threat of foreign interference. My testimony today focuses on 6 steps that can be taken now to help ensure that the 2020 election is safe, secure, and fair.

State and local election officials with help from their partners must continually evaluate their election infrastructure to ensure it is as secure as possible. Testing and auditing existing systems is essential.

At a recent meeting of the National Association of Secretaries of State, Matt Masterson, an advisor with the U.S. Department of Homeland Security, told State officials that DHS testing of State and local elections systems have found a number of concerning vulnerabilities. These included, No. 1, sharing passwords and other credentials, and using default passwords commonly known to outsiders; and No. 2, continuing to fall for phishing attacks that allow hackers to install malware, including ransomware that could paralyze Election Day operations.

As Masterson noted, the good news is that many of these issues can be easily fixed by election day. The bad news is that many local

election offices are unable to make these fixes quickly because they lack the necessary resources or IT support. The coronavirus has exacerbated the problem by forcing a number of States to divert election security funding to cover other unanticipated costs stemming from the pandemic.

As the election infrastructure is modified to account for the coronavirus or other intervening events, security and resiliency measures must be part of the design and not introduced after the fact.

In its June 2 primary election, the Washington, DC Board of Elections, inundated with complaints from voters who did not receive absentee ballots in the mail, decided as a last resort to allow a number of domestic voters to submit their ballots by email, so that their votes could be cast and counted. While the effort was well-intentioned, it put election results at risk because there is no way either for those voters to verify that their votes were recorded accurately, or to ensure that those votes were not altered in transmission by bad actors. Even if there is no actual interference with email ballots, allowing them provides fodder to foreign adversaries who could use such actions to sow doubt and confusion about the legitimacy of our elections.

We need to ensure that our elections are run as smoothly as possible so that mis- and disinformation is less likely to be effective. If our general election is plagued by significant problems, inaccurate information is more likely to find a receptive audience, as we have seen with Russia and Iran already.

Regardless of how secure our elections are, experts and officials are concerned that some voters could dismiss November's results as invalid or rigged because of mis- and/or disinformation. Voters could argue, for example, that the much-longer-than-usual time required to count an anticipated surge in mail-in ballots is direct evidence of nefarious conduct.

We must seek to flood the information space with credible, consistent election information so that voters are immunized against falsehoods. This will admittedly be challenging in light of the coronavirus and the constant change it is required. But it is doable, particularly, if Federal authorities can provide State and local election officials additional funding to publicize and explain changes to their election processes. It is essential that also partisan politics be kept out of election administration to build confidence in the integrity of the election process, and it should happen long before Election Day.

For example, Kentucky had a relatively smooth primary election, in part, due to a bipartisan agreement reached well in advance of the election between a Democratic Governor and a Republican Secretary of the State. It took a number of joint steps to help the State prepare for its primary, including allowing for unprecedented expansion of absentee voting, and allowing in-person absentee voting, which is effectively early voting.

Election officials, finally, must also have sufficient resources to plan for reasonably foreseeable contingencies. Offering robust voting-by-mail, early voting, and election-day options to minimize confusion and risks are optimal, but many jurisdictions don't currently have the resources and/or personnel to offer all of these ap-

proaches. Additional resources from Federal authorities would help enormously with administering and securing the election, but time is of the essence.

The late Congressman John Lewis once said, "Your vote is precious, almost sacred. It is the most powerful, nonviolent tool we have to create a more perfect union."

I urge Congress to do everything possible to ensure that every person who wants to exercise their right to vote can do so. Thank you.

[The prepared statement of Mr. Levine follows:]

PREPARED STATEMENT OF DAVID LEVINE

AUGUST 4, 2020

I. INTRODUCTION

Chairman Richmond, Ranking Member Katko, and Members of the Subcommittee on Cybersecurity, Infrastructure Protection & Innovation: Thank you for the opportunity to testify today on protecting the integrity of the 2020 elections during the COVID–19 pandemic.

My name is David Levine, and I am the Elections Integrity Fellow for the Alliance for Securing Democracy (ASD), a bipartisan, transatlantic initiative housed within the German Marshall Fund of the United States. ASD develops comprehensive strategies to deter and defend against authoritarian efforts to undermine and interfere in democratic institutions. Election integrity has been a core priority since our inception, and we continue to be at the forefront of efforts to raise awareness of threats and recommend legislative and technical mitigation measures.

Prior to joining ASD, I served as the Ada County, Idaho elections director, where I collaborated with the county's elected officials to plan, oversee, and administer elections for more than 250,000 registered voters across 150 precincts. Before that, I spent several years as a senior election administrator and consultant, helping administer elections in Richmond, Virginia and Washington, DC. And on behalf of the Organization for Security and Cooperation in Europe, of which the United States is a member, I have been privileged to act as an observer for a number of elections overseas.

This year, the United States has had a primary election season unlike any other. Since the primaries began, our country has endured a public health crisis that has claimed the lives of more than 150,000 people;[1] experienced substantial protests and unrest in the aftermath of George Floyd's death;[2] and conducted elections while trying to secure them from foreign adversaries, including Russia, China, and Iran.[3] State and local election officials, partner organizations, voters and other stakeholders are being forced to grapple with new election-related challenges in real time as they strive to hold safe, secure, and accessible elections. Changes to voting processes to account for the coronavirus impact the security of our elections. The steps we take to combat the coronavirus must therefore consider the threat of foreign interference, in addition to public health and election administration.

My testimony today focuses on steps that can be taken now to help ensure that the 2020 general election is safe, secure, and fair. To do this, I will address election infrastructure, information, administration, and funding.

II. ELECTION INFRASTRUCTURE

One noteworthy success from the 2020 primary elections is that there hasn't yet been any confirmed successful attack on our country's election infrastructure. I think that is a testament, at least in part, to the strides our country has made in improving our election security since the 2016 Presidential election, when we had relatively little awareness of the threats foreign actors posed to our elections. State and local election officials have subsequently become more well-versed on cybersecu-

---

[1] Norah O'Donnell. "U.S. hits 150,000 deaths," CBS News, July 29, 2020, *https://www.cbsnews.com/news/covid-united-states-150000-deaths-coronavirus/*.

[2] Derrick Bryson Taylor. "George Floyd Protests: A Timeline," The New York Times, July 10, 2020, *https://www.nytimes.com/article/george-floyd-protests-timeline.html*.

[3] U.S. Department of National Intelligence, Statement by NCSC Director William Evanina: 100 Days Until Election 2020, July 24, 2020, *https://www.dni.gov/index.php/newsroom/press-releases/item/2135-statement-by-ncsc-director-william-evanina-100-days-until-election-2020*.

rity issues, and with the assistance of Federal agencies like the Department of Homeland Security's (DHS) Cybersecurity & Infrastructure Security Agency (CISA), and a whole host of civil society organizations and private-sector actors, there is now much more information sharing and awareness of potential threats, as well as proactive measures to protect our election infrastructure than before.

That said, the work of securing the 2020 Presidential election is far from over. Below are 3 steps that election officials and their partners must continue taking to help ensure that November's 2020 election is a secure one.

First, State and local election officials, with help from their partners, must continually evaluate their election infrastructure to ensure it is as secure as possible. Testing and auditing existing systems is essential.

In June 2016, the State of Illinois experienced the first known breach by Russian actors of State election infrastructure during the 2016 election. By the end of 2018, Russian agents had successfully penetrated Illinois's voter registration database, accessed as many as 200,000 voter registration records, and exfiltrated an unknown quantity of voter registration data. And while we are not aware of any evidence that voter registration data was deleted or changed, the U.S. Senate Select Committee on Intelligence found that Russian cyber actors were in a position to modify the data they accessed.[4]

The Colorado Secretary of State's office recently announced that it is partnering with a security firm to conduct penetration tests of its election systems ahead of the Presidential vote. Trevor Timmons, the chief information officer for Colorado Secretary of State Jena Griswold, indicated that the firm's "white-hat" hackers would examine the agency's election infrastructure, including the State-wide voter registration database, the Secretary's main website, and electronic pollbooks at physical precincts for people who choose to vote in person because "We need to know [vulnerabilities]. We've got enough time that if they found anything we'd be able to respond to them."[5]

While the security of our election infrastructure, including our State voter registration databases, appears to have improved since 2016, this kind of testing still has tremendous value. At a recent meeting of the National Association of Secretaries of State, Matt Masterson, an advisor with CISA, told State officials that DHS testing of State and local election systems had found a number of "concerning" vulnerabilities. These included: (1) Sharing passwords and other credentials, and using default passwords commonly known to outsiders; and (2) continuing to fall for "phishing" attacks that allow hackers to install malware, including ransomware that could paralyze Election Day operations.[6] As Masterson noted, the good news is that many of these issues can be easily fixed by Election Day. The bad news is that many local election offices are unable to make these fixes quickly because they lack the necessary resources or IT support. The coronavirus has exacerbated the problem by forcing a number of States to divert election security funding to cover other unanticipated costs stemming from the pandemic.[7]

Second, as the election infrastructure is modified to account for the coronavirus or other intervening events, security and resiliency measures must be part of the design and not introduced after the fact.

In its June 2 primary election, the Washington, DC Board of Elections (DCBOE)—inundated with complaints from voters who did not receive requested absentee ballots—decided as a last resort to allow a number of domestic voters to submit their ballots by email so that their votes could be cast and counted.[8] While the effort was well-intentioned,[9] it put the election results at risk because there is no way either

---

[4] U.S. Congress, Senate, Select Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 106 U.S. Election, Volume 1: Russian Efforts Against Election Infrastructure with Additional Views, 116th Cong., 1st sess., 2019, 4 [sic], *https://www.intelligence.senate.gov/sites/default/files/documents/Report__Volume1.pdf*.

[5] Benjamin Freed. "Colorado official details plan for penetration testing of election systems," StateScoop, July 28, 2020, *https://statescoop.com/colorado-official-details-plans-for-penetration-testing-of-election-systems/*.

[6] Pam Fessler. "With November Approaching, Election Officials Still Face Safety, Security Fears," NPR, July 24, 2020, *https://www.npr.org/2020/07/24/894736356/with-november-approaching-election-officials-still-face-safety-security-question.*

[7] Matthew Vann. "Some cash-strapped States turn to election security funds to fight COVID–19," ABC News, April 6, 2020, *https://abcnews.go.com/Politics/cash-strapped-states-turn-election-security-funds-fight/story?id=69940136.*

[8] Alexa Corse. "D.C. Lets Voters Submit Ballots by Email After Mail Problems," The Wall Street Journal, June 3, 2020, *https://www.wsj.com/articles/d-c-lets-voters-submit-ballots-by-email-after-mail-problems-11591211518.*

[9] In addition to trying to ensure that additional voters could cast ballots in a timely manner, the DCBOE was reported to have required people who voted by email to submit an affidavit verifying their identity. The DCBOE also indicated that it planned to call everyone who voted

for those voters to verify that their votes were recorded accurately, nor is there a way to ensure that those votes were not altered in transmission by bad actors.[10]

And even if there is no actual interference with emailed ballots, allowing them provides fodder to foreign adversaries who could use such actions to sow doubt and confusion about the legitimacy of our elections. That is not idle speculation—it has been voiced by authoritative sources ranging from the Senate's Select Committee on Intelligence,[11] to the National Academies of Science, Engineering, and Medicine,[12] CISA, the Election Assistance Commission (EAC), the Federal Bureau of Investigation, and the National Institutes of Standards of Technology.[13]

While the DCBOE has already said that it does not plan to allow email voting in November, the situation it found itself in is one that other jurisdictions could face, especially if COVID–19 continues to make in-person voting challenging, requests to vote-by-mail continue to multiply, and additional funds are not made available.[14] It is important that contingency plans for scenarios such as those above be developed well in advance of November and rely on proven, secure, resilient voting processes.

Finally, State and local officials should continue to be offered help in securing their election infrastructure before November.

Federal agencies such as CISA and the EAC have resources available to help detect and fix flaws, provide security training, and share best practices for securing our elections. Some civil society organizations can act quickly to help secure elections from the bottom up.[15] With fewer than 100 days before November 3, one of the best ways such organizations could assist election officials at this juncture would be to help identify poll workers who are willing to assist with in-person voting at a time when the coronavirus is still expected to be circulating.

But civic action and commitment are not enough. The single most important assistance that election officials could use at this juncture is additional Federal funding. Congress provided $400 million to the States for election assistance in March as part of the Coronavirus Aid, Relief and Economic Security (CARES) Act. That was an important first step that has helped enable many States and localities to go to greater lengths to try and conduct accessible, secure elections during the pandemic. That said, as a recent report put out by a(n) ideologically diverse group of organizations, including ASD, Brennan Center for Justice at NYU Law, the R Street Institute and University of Pittsburgh Institute for Cyber Law, Policy and Security noted, $400 million isn't enough to cover the remaining 2020 election costs in Georgia, Michigan, Missouri, Ohio, and Pennsylvania, let alone the costs of the other 45 States and entities like DC, Puerto Rico, and the U.S. Virgin Islands.[16] Without further Federal assistance, the likelihood of there being significant issues in the November general election will go up. States and local governments across the country are facing severe budget challenges as a result of COVID–19.[17] Not surprisingly, dealing with the disease itself gets first priority, but that means that many are not in a position to cover the unanticipated election costs arising from the virus.

---

by email to verify that was how they submitted a ballot. Joseph Marks. "The Cybersecurity 202: D.C.'s use of email voting shows what could go wrong in November," The Washington Post, June 4, 2020, *https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/06/04/the-cybersecurity-202-d-c-s-use-of-email-voting-shows-what-could-go-wrong-in-november/5ed7dd38602ff12947e83396/*.

[10] Ibid.

[11] U.S. Congress, Senate, Select Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 106 U.S. Election, Volume 1: Russian Efforts Against Election Infrastructure with Additional Views.

[12] The National Academies of Sciences, Engineering, and Medicine, Securing the Vote: Protecting American Democracy, 2018, *http://nap.edu/25120.*

[13] The Cybersecurity and Infrastructure Security Agency, the Election Assistance Commission, the Federal Bureau of Investigation and the National Institute of Standards and Technology, Risk Management for Electronic Ballot Delivery, Marking, and Return, May 2020, *https://s.wsj.net/public/resources/documents/Final__%20Risk__Management__for__Electronic-Ballot__05082020.pdf?mod=article__inline*.

[14] Marks, "The Cybersecurity 202: D.C.'s use of email voting shows what could go wrong in November."

[15] U.S. Cyberspace Solarium Commission, March 2020, *https://www.solarium.gov/*.

[16] Christopher R. Deluzio, Elizabeth Howard, David Levine, Paul Rosenzweig, Derek Tisler, "Ensuring Safe Elections: Federal Funding Needs for State and Local Governments During the Pandemic," Brennan Center for Justice, April 30, 2020, *https://securingdemocracy.gmfus.org/wp-content/uploads/2020/05/Ensuring-Safe-Elections.pdf*.

[17] Ibid.

III. ELECTION MIS- AND DISINFORMATION

Regardless of how secure our elections are, many election experts and officials are concerned that some voters could dismiss November's results as invalid or rigged because of mis- and/or disinformation. Voters could argue, for example, that the much-longer-than-usual time required to count an anticipated surge in mail-in ballots is prima facie evidence of nefarious conduct. While most of us know that such allegations are not true, similar rhetoric is already being amplified by foreign adversaries, such as Russia and Iran, to diminish confidence in the election results and undermine our democracy.[18] In response, we need to do at least two things.

First, we need to ensure that our elections are run as smoothly as possible, so that mis- and disinformation is less likely to be effective. If our general election is plagued by significant problems, inaccurate information is more likely to find a receptive audience.

For example, during the February 3, 2020 Iowa Democratic caucuses—which were administered by political party officials, not election officials—the new app that the Iowa Democratic Party used to report caucus results did not work as planned,[19] resulting in a system-wide meltdown.[20] That provided enough of an opening for a conspiracy theory to go viral and be amplified by accounts with Russian links. This conspiracy theory accused Robby Mook (Hillary Clinton's 2016 campaign manager) of developing Iowa's mobile app to rig the Democratic primary against Senator Bernie Sanders (Secretary Clinton's former rival)—even though Mr. Mook had not developed (or even heard of) the app.[21]

Even reasonable decisions about our voting processes can be become fodder for foreign adversaries.[22] In April, New York tried to become the first State to cancel its Presidential primary over coronavirus concerns, a move that was subsequently overturned[23] by a Federal court. Never wanting to miss an opportunity to cry foul, Russian actors seized on the move to highlight domestic "outrage" at the change and suggest that it constituted a "blatant coronation" of Vice President Joe Biden at the expense of Senator Bernie Sanders.[24] Reasonable minds can differ about the State Board of Election's (SBE) decision to cancel the Presidential primary, but the transparent, legal process that played out after that decision stood in stark contrast to the lack of recourse or due process offered by authoritarian regimes like Russia.

Second, we must seek to flood the information space with credible, consistent election information so that voters are 'immunized' against falsehoods.

This will admittedly be challenging in light of the coronavirus—because many voters are likely to be voting in a different manner than they have previously, and election officials have been forced to make continuous changes to their voting processes as the pandemic evolves. But it is doable, particularly if Federal authorities can: (1) Provide State and local election officials additional funding to publicize and explain changes to their voting processes; and (2) communicate as much information about election threats as possible to election officials and the public. Flooding the space with this kind of information will also sensitize journalists, candidates, and the public to the fact that we may not know the election results immediately and that this is not, in and of itself, proof of malfeasance.

---

[18] Clint Watts. "Triad of Disinformation: How Russia, Iran & China Ally in a Messaging War Against America," Alliance for Securing Democracy, May 15, 2020, *https://securingdemocracy.gmfus.org/triad-of-disinformation-how-russia-iran-china-ally-in-a-messaging-war-against-america/*.

[19] David Levine. "The Election Official's Handbook: Six steps local officials can take to safeguard America's election systems," Alliance for Securing Democracy, February 13, 2020, *https://securingdemocracy.gmfus.org/wp-content/uploads/2020/02/The-Election-Officials-Handbook-2.pdf*.

[20] Shane Goldmacher and Nick Corasaniti. "'A Systemwide Disaster': How the Iowa Caucuses Melted Down," The New York Times, February 04, 2020, *https://www.nytimes.com/2020/02/04/us/politics/what-happened-iowa-caucuses.html*.

[21] Nicole Perloth. "A Conspiracy Made in America May Have Been Spread by Russia," The New York Times, June 15, 2020, *https://www.nytimes.com/2020/06/15/technology/coronavirus-disinformation-russia-iowa-caucus.html*.

[22] Jessica Brandt. "To Ensure a Healthy Election in a Pandemic, First Prepare the Information Space," Alliance for Securing Democracy, May 14, 2020, *https://securingdemocracy.gmfus.org/to-ensure-a-healthy-election-in-a-pandemic-first-prepare-the-information-space/*.

[23] Katelyn Burns, "The New York State Presidential primary is back on a Federal court ruling," Vox, May 6, 2020, *https://www.vox.com/policy-and-politics/2020/5/6/21249108/new-york-state-presidential-primary-back-on-Federal-court-ruling*.

[24] Brandt, "To Ensure a Healthy Election in a Pandemic, First Prepare the Information Space."

IV. ELECTION ADMINISTRATION

The 2020 primary elections gave many States an opportunity to conduct at least one election during the pandemic prior to November. There are at least 3 important takeways from these elections that can be applied to November.

First, it is essential that partisan politics be kept out of election administration to build public confidence in the integrity of the election process, and this must happen long before Election Day.

Wisconsin's April 7 primary illustrated what can go wrong when State leaders refuse to act on a timely basis, and ended up conducting in-person voting in the middle of the State's coronavirus outbreak. There were not enough poll workers and dueling court cases sowed confusion about absentee voting, contributing to thousands of missing or nullified ballots.[25] In Milwaukee, where roughly 4 in 10 residents are Black, officials closed all but 5 of the city's 180 polling places, forcing thousands of voters to congregate at a handful of voting sites. Many voters were forced to choose between risking their health to cast a ballot or staying at home and forfeiting their vote.[26]

Such mishaps provide openings to adversaries such as Russia, which has targeted African-Americans with disinformation operations since the 2016 Presidential election,[27] as well as China and Iran, both of whom have used the coronavirus in an effort to undermine our democracy.[28]

In contrast, Kentucky had a relatively smooth primary election despite early fears of turmoil, in part due to a bipartisan agreement reach well in advance of the election between the Democratic Governor, Andy Beshear, and the Republican Secretary of State, Michael Adams. Beshear and Adams took a number of joint steps to help the State prepare for its primary, including allowing for an unprecedented expansion of absentee voting and allowing "in-person absentee voting", which is effectively early voting and does not typically take place in Kentucky.[29]

Second, election officials must have sufficient resources to plan for reasonably foreseeable contingencies.

From an election administration, election security, and public health standpoint, it would be optimal if as many voters as possible voted before Election Day, either in person or from home. That increases the time and choices available to address any issues that may arise, such as malfunctioning voting equipment, long lines at voting locations or unexpected delays in the mail service. But whatever election officials do, many people will likely insist on voting in-person on Election Day regardless of the pandemic—a development Georgia experienced first-hand during its primary.

After twice postponing its primary due to the coronavirus, Georgia substantially modified its election process to try to account for the virus. It took the unprecedented step of mailing out absentee ballot applications to all of the 6.9 million active registered voters in Georgia to encourage more mail-in voting,[30] and while a much higher percentage of ballots were cast by mail than in previous elections, more than half of all votes were still cast in-person;[31] many of those voters had a difficult experience. For example, voters in parts of metro Atlanta waited in lines for more than 4 hours on Election Day as election officials conducted an election with fewer voting

---

[25] Amber Phillips. "Wisconsin's decision to hold its primary is threatening to become a worst-case scenario for elections amid a pandemic," The Washington Post, April 6, 2020, *https://www.washingtonpost.com/politics/2020/04/03/wisconsins-decision-go-ahead-with-its-primary-is-glimpse-worst-case-scenario-elections-during-coronavirus/*.

[26] Li Zhou and Ella Nilsen. "Liberal challenger Jill Karofsky wins a seat on the Wisconsin Supreme Court," Vox, April 13, 2020, *https://www.vox.com/2020/4/13/21219284/jill-karofsky-wisconsin-supreme-court*.

[27] U.S. Congress, Senate, Select Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media, 116th Cong., 1st sess., 2019, *https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf*.

[28] Watts. "Triad of Disinformation: How Russia, Iran & China Ally in a Messaging War Against America."

[29] Zach Montellaro. "Coronavirus threatened to make a mess of Kentucky's primary. It could be a model instead," Politico, July 4, 2020, *https://www.politico.com/news/2020/07/04/coronavirus-voting-kentucky-primary-348611*.

[30] Alexa Corse. "Voting by Mail to Face Biggest Test Since Pandemic Started," The Wall Street Journal, June 1, 2020, *https://www.wsj.com/articles/voting-by-mail-to-face-biggest-test-since-pandemic-started-11591003801*.

[31] Mark Niesse, "Turnout broke records in Georgia primary despite coronavirus threat," The Atlanta Journal-Constitution, Updated July 11, 2020, *https://www.ajc.com/news/state--regional-govt--politics/turnout-broke-records-georgia-primary-despite-coronavirus-threat/G1JnSflr1YMOU06btlnbVJ/*.

machines in polling places, fewer places to vote, and fewer experienced poll workers because of the pandemic.[32]

Offering robust voting-by-mail, early voting, and Election Day options to minimize confusion and risk are optimal, but many jurisdictions don't currently have the resources and/or personnel to offer these approaches. For example, Maryland Governor Larry Hogan decided last month that the State would hold a traditional election in November, offering many in-person voting locations and allowing voters to vote in their customary precincts. At the end of July, the President of the Maryland Association of Election Officials indicated that local election boards are experiencing tremendous difficulty in recruiting Election Day poll workers, with roughly 13,000 vacant positions State-wide.[33] On July 27, Howard County, Maryland Election officials reported that 491 people had signed up to serve as Election Judges for the general election, about a third of the number needed. By the time the county election board met soon thereafter, the number of confirmed Election Judges had dropped to 12 as Judges hurriedly withdrew their pledges to participate in the face of the pandemic.[34]

Additional resources from Federal authorities will help enormously with the administration of the 2020 Presidential election, but with fewer than 100 days to go until November 3, time is of the essence. As other experts have noted, more funding could enable election officials to procure personal protective equipment (PPE) to make in-person voting safer; purchase additional mailing, ballot, and postage supplies in preparation for the anticipated surge in absentee voting; conduct robust voter education campaigns so that voters are aware of how to vote safely; recruit and train needed poll workers; and identify additional polling places.[35]

New funding could also mitigate any cyber or technical-related problems that would impact the administration of the general election. While jurisdictions in 41 States and the District of Columbia use electronic pollbooks (EPBs) to verify voter eligibility at polling places, only 12 States and DC appear to require paper backups in case the EPBs malfunction.[36] More funds could help more jurisdictions obtain paper back-ups for use if their EPBs become inoperable due to a cyber attack or technical glitch.[37] To cite just one other example, localities with electronic voting machines could use funding to purchase extra provisional ballots in the event that their voting machines go down during the general election so that voters don't have to wait for extended periods of time following a system failure.[38]

V. CONCLUSION

Administering and securing a Presidential election is no small feat in ordinary times, and these times are anything but ordinary. Success will require a coordinated Nation-wide effort. Congress needs to provide election officials with additional funding to help them administer and secure the November election.

Federal officials involved in helping secure and administer our country's elections need to continue to actively support the efforts of State and local election officials to, among other things, mitigate any efforts by foreign adversaries to interfere in our elections. And civil society and private sector actors need to work with Government entities to help fill any remaining gaps.

---

[32] Stephen Fowler, "'It Was Very Chaotic': Long Lines, Voting Machine Issues Plague Georgia Primary," NPR, June 9, 2020, *https://www.npr.org/2020/06/09/873054620/long-lines-voting-machine-issues-plague-georgia-primary.*

[33] Zach Montellaro, "Coronavirus creates election worker shortage ahead of November," Politico, July 31, 2020, *https://www.politico.com/news/2020/07/31/coronavirus-election-worker-shortage-389831.*

[34] Emily Opilo and Talia Richman, "Local election officials in Maryland look at slashing number of polling places due to election judge shortage," The Baltimore Sun, July 29, 2020, *https://www.baltimoresun.com/politics/bs-md-pol-polling-place-consolidation-Governor-hogan-2020-0729-4s3j7gq3afb3va57iwxpa24lcy-story.html.*

[35] Statement of Kristen Clarke, Lawyers' Committee for Civil Rights Under Law, Senate Committee on Rules and Administration Hearing on "2020 General Elections Preparations," July 22, 2020, *https://www.rules.senate.gov/imo/media/doc/Testimony_Clarke.pdf.*

[36] Edgardo Cortes, Elizabeth Howard, Lawrence Norden, Gowri Ramachandran, and Derek Tisler, "Preparing for Cyberattacks and Technical Problems During the Pandemic: A Guide for Election Officials," Brennan Center for Justice, June 5, 2020, *https://www.brennancenter.org/our-work/research-reports/preparing-cyberattacks-and-technical-problems-during-pandemic-guide.*

[37] David Levine and Matthew Weil. "20 for 20: 20 Ways to Protect the 2020 Presidential Election," Alliance for Securing Democracy and Bipartisan Policy Center, May 20, 2020, *https://securingdemocracy.gmfus.org/wp-content/uploads/2020/06/20-for-20-20-Ways-to-Protect-the-2020-Presidential-Election.pdf.*

[38] Ibid, 6.

Voters have a part to play as well. They must plan now for how they will vote in November. And if they want to vote in-person, they should give serious thought to serving as a poll worker.

The late Congressman John Lewis once said, "Your vote is precious, almost sacred. It is the most powerful nonviolent tool we have to create a more perfect union."

We urge Congress to do everything possible to ensure that every person who wants to exercise their right to vote can do so.

Thank you.

Mr. RICHMOND. Thank you, Mr. Levine.

We now recognize Ms. Albert to summarize her statement for 5 minutes.

STATEMENT OF SYLVIA ALBERT, DIRECTOR OF VOTING AND ELECTIONS, COMMON CAUSE

Ms. ALBERT. Good morning. Thank you, Chairman Richmond, for inviting me to testify today. Thank you to Chairman Richmond, Ranking Member Katko, and all Members of the subcommittee, for holding this critically important hearing.

My name is Sylvia Albert, and I am the director of voting and elections at Common Cause, a National nonpartisan watchdog organization with 1.2 million supporters and more than 25 State chapters. For nearly 50 years, Common Cause has been holding power accountable through lobbying, litigation, and grassroots organizing. Common Cause fights to get big money out of politics, enhance voting rights, foster an open, free, and accountable media, strengthen ethics laws to make Government more responsive to the people, ensure a fair Census, and stop gerrymandering.

The COVID–19 pandemic presents an unprecedented challenge to our democracy. We have long known that our decentralized voting systems mean that voters have vastly different voting experiences, depending on where they live. While the world varies, there is one thing that is uniform. There is no such thing as a perfect election. Long-standing disparities, including long lines, polling place closures, a ballot rejection rate, particularly in Black and Brown communities, are now exacerbated by the COVID–19 pandemic. The chasm between those with access to ballots and those with significant barriers to that access is growing larger. Voters of color, young voters, and first-time voters are on the losing end. Without proper funding, the problems seen in previous elections are going to be just the tip of the iceberg this November.

While only a small percentage of the electorate participates in primaries, the 2020 primary season is a preview of the problems to come. There is no single solution to ensure a safe and secure election. However, by understanding this compounding issue, we can work to eliminate the barriers voters face. I want to highlight some of these issues, but for more detailed proof in my written testimony.

In nearly every State that voted since the pandemic, we saw a dramatic increase in the use of mail-in ballots. One common issue was that ballots were mailed too late and some voters did not receive them at all. In many States, the infrastructure to process requests and produce ballots did not handle this huge increase.

Expecting voters to vote-by-mail, election officials overconsolidated poll locations. When they were unable fulfill the requests for

absentee ballots, voters were forced to vote in person at a small number of polling locations that were, therefore, overrun.

For example, Pennsylvania's 2 most populous counties, Philadelphia and Allegheny, shifted for more than 2,100 polling places to fewer than 500, resulting in confusion and long lines. In addition, the polling places chosen for consolidation were not done equitably or with regard to the disparity of mail-in ballot applications.

In addition, voting machine failures led to disenfranchisement. Problems were particularly wide-spread in Georgia, ranging from machines not working to polling locations not having enough machines, or when machines go down, there is not—there was not enough paper ballots available to meet the demand. As a result, voters had no choice but to wait in line or not vote.

To be clear, with the correct implementation of resources, running an election that gives voters safe and secure options to vote-by-mail and in person if it is possible, but time is running out.

During an election, officials have long tried to make voting more difficult for Black and Brown communities. Impacts in these efforts are greater exacerbated in a global pandemic. However, there are solutions that will create systemic change.

Most importantly, it is going to take significantly more resources for States to run effective elections in the COVID–19 environment. To address each of the problems discussed, States need not only to adopt the policies, but also to have the funds necessary to execute those policies. One study estimates this cost to be $4 billion. Senate Republicans must follow the House's lead and allocate $3.6 billion in election funding.

Second, even prior to the pandemic, 70 percent of election officials reported that it was difficult to staff polling locations. In addition, many traditional polling locations are no longer available.

Members of Congress can help recruit poll workers and find new polling locations by putting out requests on social media, doing PSAs, and using their extensive network to encourage this important civic engagement.

Third, H.R. 1 includes many strong protections for voters, including the Voter Empowerment Act, which Congressman Lewis long championed. We appreciate Chairman Richmond cosponsoring and voting for H.R. 1 when it passed the House in March 2019, and we continue to strongly urge Senator McConnell to bring it up for a vote in the Senate.

Finally, as we approach the 55th anniversary of the Voting Rights Act later this week, I can't think of a better way to honor the life of Congressman John Lewis than by having the Senate follow the House's lead and pass the John Lewis Voting Rights Advancement Act.

Voters should not be forced to choose between their health and their right to vote. With the election less than 3 months away, we need Congress to act now. In order to ensure the 2020 election is safe, secure, accessible, and fair, Congress must invest so States and localities can implement critical voting system changes that this pandemic demands. Thank you.

[The prepared statement of Ms. Albert follows:]

PREPARED STATEMENT OF SYLVIA ALBERT

AUGUST 4, 2020

INTRODUCTION

Thank you, Chairman Richmond, for inviting me to testify before the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation. Thank you to Chairman Richmond, Ranking Member Katko, and all Members of the subcommittee for holding this critically important hearing. My name is Sylvia Albert, and I am the director of voting and elections at Common Cause, a National nonpartisan watchdog organization with 1.2 million supporters and more than 25 State chapters. For nearly 50 years, Common Cause has been holding power accountable through lobbying, litigation, and grassroots organizing. Common Cause fights to get big money out of politics, enhance voting rights, foster an open, free, and accountable media, strengthen ethics laws to make Government more responsive to the people, ensure a fair Census, and stop gerrymandering.

Common Cause was founded by John Gardner, a Republican, at a time when Republicans and Democrats worked together on the most pressing issues of the day. During the 1970's, Common Cause worked with many Members of Congress—Democrats and Republicans alike—who put country over party, and we were able to help pass major democracy reforms that sought to correct some of the most egregious abuses of power, including the Federal Election Campaign Act, the Ethics in Government Act, and Voting Rights Act reauthorizations, which are still extremely consequential to this day.

The COVID–19 pandemic presents an unprecedented and different kind of challenge to our democracy. Under normal circumstances, conducting elections is a collection of choreographed large-scale productions. With more than 10,000 election jurisdictions Nation-wide, our decentralized voting system is in the hands of local and State election officials. While the mechanisms and rules vary across the country, there is one thing that is uniform—there is no such thing as a perfect election. Voters' experiences reveal the cracks in the foundation that infringe on their right to vote. These cracks can be seen in the adoption of policies that create significant barriers to voting for certain individuals, especially Black and Brown voters. They can be seen in election administration choices that lead to long lines, polling place closures, and ballot rejections at higher rates in Black and Brown communities. These cracks have always existed. The crisis we are currently facing is exposing the weaknesses in the system that have previously been hidden from much of the electorate. COVID–19 is exacerbating these cracks and widening the chasm between those with access to the ballot and those with significant barriers to that access. Without proper funding, guidance, and preparedness, the problems seen in previous elections are going to be just the tip of the iceberg this November.

2020 PRIMARIES

The 2020 primary season gave us a small preview of the problems to come. Keeping in mind that only a small percentage of the electorate participates in primaries, we know that the issues we saw will grow exponentially if proper preparation isn't made before November. The problems we saw did not exist in a vacuum. Each issue, from poor election management, to faulty voting machines, to lack of poll workers, affects each other. There is neither one problem nor one solution to ensure a safe, secure, free, and fair election. However, by understanding the compounding issues, we can work to eliminate the barriers voters face from making their voices heard.

As a member of the Election Protection coalition, a National group of National and local organizations that help voters who experience problems casting their ballots through a suite of vote protection hotlines and other tools, we at Common Cause have seen many of these issues play out not only in the last few months, but in all recent elections. The COVID–19 pandemic has only made problems worse.

Polling place consolidations

As State and local governments dealt with a dramatic increase in mail-in voting, a shortage of poll workers, and attempts to follow public health guidelines, we saw many polling place consolidations across the country. Overconsolidation in the current environment can have drastic results.

Pennsylvania's two most populous counties, Philadelphia and Allegheny, shifted more than 2,100 polling places open in a typical election to fewer than 500, resulting in confusion, long lines, and inaccessibility for voters with disabilities. In addition, the choices with respect to consolidation were not done equitably, or with regard to the disparities in mail ballot applications. In some counties, such as Allegheny

County, mail ballot applications were more likely received from white voters, so non-white voters were faced with voting in-person at more consolidated locations.

In New Mexico, only 381 out of the 548 polling locations were open, which was particularly challenging for the Native population that is suffering from COVID–19 at a much higher rate than the rest of the State. In Rhode Island, only 47 polling places of the 144 that were open in 2016 were available to voters. In Washington, DC, only 20 of the 144 polling places from 2016 were open. In Nevada's June 9 primaries, which was conducted primarily by mail, only 3 polling places were open for the Las Vegas area's 1.3 million voters, contributing to long lines. In Richland County, SC, polling place consolidation coupled with poll worker shortages led to long lines for the State's June 9 primary. Polling place consolidations in Wisconsin for the State's April 7 elections received wide-spread media coverage because of the drastic changes. In Milwaukee, just 5 of the normal 180 voting locations were open, and in Green Bay, only 2 out of the normal 31 were open.

These are just not facts and figures either. These problems affect real people and voters across the country. Amina M., a Wisconsin voter who had given birth only 2 weeks earlier, waited over 2 hours in line in Milwaukee, fearing for her health. Layato G, a voter in Fulton County, Georgia, told Common Cause her story during our election protection efforts, and her story was not unique. She requested an absentee ballot, but it never arrived so she was forced to vote in person. When she arrived at her polling place, she found out there were problems with the voting machines and ended up waiting in line to vote for 3 hours. When she was finally able to cast her ballot, she was forced to vote on a provisional ballot because she had been marked as an absentee voter in the pollbook. Because of this confusion, she left the polling place without assurance that her vote would even be counted.

When coupled with the roll-out of new vote-by-mail procedures, election officials' inability to process absentee ballot applications in a timely manner, new voting machines, a lack of voter education, and a global pandemic, long lines and confusion were a foreseeable outcome of overconsolidation. Again, no issue exists in a vacuum. Decisions around polling place closures must be made in consideration of all of the other pieces of election administration, and the needs and wants of the community. Closing a polling location should never be the first option considered in changes to election administration.

Administration of Increased Vote by Mail Usage

In nearly every State that voted since the COVID–19 pandemic outbreak, we saw a dramatic increase in the use of mail-in ballots. In Washington, DC, more than 60 percent of ballots cast in the 2020 primary were by mail, compared to just 7 percent in the 2016 primary. In Iowa, 410,000 people voted absentee in the 2020 primary, compared to 38,000 in the 2016 primary. In Pennsylvania, more than 1.8 million people requested absentee ballots, compared to just over 100,000 from 4 years ago, thanks to Pennsylvania's recent law expanding absentee ballot use. In Georgia, election officials saw a 2,500 percent increase in voting-by-mail from the 2016 primary. In West Virginia, more than 262,000 voters requested an absentee ballot compared to 6,700 requests in 2016.

Unfortunately, States were not equally prepared to handle this influx. Voting-by-mail is a solution that has been tried and tested in States across the country, but many of the primary States were trying to implement and process a level of mail-in voting that took Colorado, Oregon, Washington, and Utah years to get to. To be clear, with the correct implementation, administration, and resources, running an election mostly by mail is possible, but time is running out, and States must act now.

The challenges we saw with voting-by-mail varied from State to State. One common issue we saw was that ballots were mailed too late to voters and that some voters did not receive them at all. In many of the States that recently expanded vote-by-mail options because of COVID–19, the infrastructure to process requests and produce ballots was not fully implemented to deal with the huge increase of mail-in ballot requests. Expecting voters to use the mail, election officials over-consolidated polling locations. When they were unable to fulfill the requests for absentee ballots, voters were forced to vote in person at a small number of polling places that were therefore overrun.

In Maryland, for example, ballots were mailed to all of the State's 3.5 million registered voters, but at least 1 million of those ballots were delayed in Baltimore City and Montgomery County. In both of those localities, people of color make up a majority of the population. In Pennsylvania, the complaint heard overwhelmingly from voters was that they requested their absentee ballot, had not received it, and were risking their health to vote in person. Indiana, Rhode Island, and Georgia had similar challenges with ballots being mailed late.

Another issue with rapidly expanding mail-in voting are the use of strict return deadlines, such as Indiana's deadline for voters to drop off their ballots that they could or wish not to mail by 12 p.m. on Election Day, even though the polls didn't close until 6 p.m. In Virginia, over 5 percent of absentee ballots were rejected for arriving after Election Day. For Pennsylvania's June 2 primary, the State's inability to process absentee ballot applications and provide voters with an absentee ballot led Governor Tom Wolf to extend the deadline for receiving mail-in ballots in some counties until Tuesday June 9 as long as they were postmarked by Election Day. As a result, tens of thousands of ballots were counted that would have been rejected.

As voters exercise their right to vote in a new manner, there are bound to be mistakes made. There is a learning curve, and implementation which educates and assists voters is vital. Unfortunately, without this, voters using mail-in voting saw their ballots rejected at high rates. In the April primary in Wisconsin, 23,000 ballots were rejected, mostly because voters or their witness missed one line on the form. These voters did not receive notice of the mistake or given an opportunity to address it—their votes were simply not counted. Wisconsin's experience is not unique. In New York, as many as 28 percent of ballots in parts of Brooklyn were rejected. Seven percent of absentee ballots were rejected in Kentucky's primary and 6,700 Nevada voters had their ballots rejected because officials could not verify signatures. These ballot rejections do not affect all communities equally. Disproportionate numbers of young people, people of color, and first-time voters have their ballots rejected. We must do more to ensure that voters can vote a ballot and have confidence that it will be counted.

While all the issues we saw with mail-in voting can be solved by November with proper funding, planning, and processes, we should not lose sight of the dramatic increases in people wanting to vote-by-mail, which is a good thing. It is clear that many people want to vote-by-mail given the COVID–19 pandemic, and now election officials must make the appropriate changes to ensure they are prepared to handle a dramatic increase in mail-in ballot requests for November. State and Federal lawmakers must also provide the adequate resources to make this happen, and implement policies that notify voters of any issues with their ballots, and allow them the opportunity to cure.

Technology Problems

The pandemic also coincided with the rollout of new voting equipment in various States, such as Georgia and Pennsylvania. While States with new equipment were not the only ones to encounter problems, their problems were more severe and widespread. In deploying any machinery during elections, jurisdictions must have resiliency plans to deal with unforeseen events while protecting voters' access. Election jurisdictions that only deploy machines to vote must have emergency ballots and provisional paper ballots on hand in the event that the primary voting system fails and no one can vote or only a few people can vote at a time. Unfortunately, during the primary elections, machine failures and a lack of paper backup ballots led voters to be disenfranchised.

Several States, including Georgia, Pennsylvania, and Indiana, saw voting machine glitches and failures which contributed to further long lines. Voting machine problems in Georgia were particularly a wide-spread problem. Issues ranged from machines not working to polling locations not being staffed with enough machines, both which contributed to long lines. Unfortunately, election officials were warned that this would happen and did not listen. In February, Common Cause and the Brennan Center for Justice submitted comments to the office of Secretary of State Brad Raffensperger with specific recommendations on managing the 2020 elections. Included in these comments was both a call for more voting machines in polling locations and a clear warning that Georgia's new voting machines could fail on Election Day and that emergency back-up paper ballots were needed. Regardless of the warning, these actions were not taken. When machines went down, there were not enough paper ballots available to meet the demand, despite a legal settlement in 2019 that required greater numbers of paper emergency ballots be available. Polling places did not have "ballot on demand" printers that could print out ballots once the original supply of paper ballots was depleted. As a consequence of the shortage, voters had no choice but to wait in line or not vote.

Lack of Poll Workers

A dearth of poll workers is a long standing problem in the United States that has been exacerbated by COVID–19. In the 2018 Election Administration and Voting Survey, 70 percent of election officials reported that it was difficult to staff polling locations with an adequate number of poll workers. These poll workers, with an av-

erage age of 60, are overwhelmingly at high risk for COVID–19 and unable to work the polls without danger.

David B. of Kentucky is another voter Common Cause contacted in our election protection efforts. David was a long time poll worker, but decided he should not work the polls in the 2020 primary election because, as an older American, he was more vulnerable to COVID–19. David is not alone in the thousands of poll workers across the country who rather not expose themselves to this pandemic—and although we desperately need poll workers like David, we cannot force people to choose between their health and the willingness to volunteer.

As mentioned earlier, all these problems play off one another. When a significant number of voters who requested absentee ballots but did not receive them decided to vote in person, they voted in consolidated polling places, some with faulty voting equipment and a shortage of poll workers, all of which led to long lines for voters. In some cases, like in Georgia, the poll worker shortages and confusion over polling place consolidation led to voting locations not opening on time on Election Day.

SOLUTIONS

As election experts can attest, the majority of these problems are not new. Certain election officials have long tried to make voting more difficult for Black and Brown communities. It is especially appalling, though, that in the midst of a global pandemic, certain election officials are trying to suppress the votes and voices of largely Black and Brown communities. In many cases, the coronavirus pandemic is simply exposing these problems for all to see. It is also clear that there is neither one problem nor one solution to problems witnessed in the primaries. However, there are several short-term solutions, as well as a number of legislative solutions that would get to the root of many of these problems and create systemic change.

Members of Congress can help recruit poll workers and find new polling locations.—Given the significant shortage of poll workers this year, Members of Congress are encouraged to use various platforms to help recruit new poll workers. Putting out requests on social media, doing PSAs, and using their extensive email lists can be effective ways to attract new poll workers. Additionally, because some in-person polling locations that have previously been used may no longer be conducive to social distancing, Members of Congress can play an important role in identifying and connecting with venues in their district, such as sports stadiums and other large buildings that could provide social distancing for voters, that could serve as polling locations.

Additional election funding.—As many States and localities face huge budget deficits caused by the pandemic, our democracy is not immune. Because many elections officials essentially have to prepare for 2 different elections (one conducted by mail and one for in-person voting) this November, States and localities need additional resources to ensure no one is disenfranchised. To address each of the problems discussed above, States need not only to adopt good policies, but also have the funds necessary to execute those policies. The CARES Act passed and signed into law in March provided $400 million for States to administer their elections, but it is going to take significantly more resources for States to run efficient elections in the COVID–19 environment. One study estimates the cost of the 2020 election during the COVID–19 pandemic to be $4 billion.

In May, the U.S. House passed the HEROES Act, which includes an additional $3.6 billion in election funding, a modest investment in our democracy to help States and localities prepare to run their elections during the pandemic. It was unconscionable that the recently released "HEALS Act" from Senate Republicans contained no funding for our elections, yet included billions of dollars for fighter jets and other extraneous causes. Senate Republicans must immediately pass $3.6 billion in election funding to ensure that hundreds of thousands or even millions of voters are not disenfranchised this year. With less than 3 months until the November election, Congress must act now so States have enough time to make the necessary changes and plans, recruit and train workers, buy equipment, and do outreach to the public about new voting processes.

H.R. 1, the For the People Act.—H.R. 1 includes many extremely strong protections for voters, such as on-line voter registration, same-day (also known as "Election Day") registration, and automatic voter registration to ensure that voters can safely and securely register to vote during the pandemic. Each of these provisions allows for voters to have more opportunities, in the face of challenges (brought on by COVID for some, but always in existence for others) to be able to vote and have confidence that it will count. The For the People Act also includes the Deceptive Practices and Voter Intimidation Prevention Act to deter bad actors from trying to spread false information about voting. And importantly, the For the People Act in-

cludes the Voter Empowerment Act, which Congressman Lewis long championed. We very much appreciate Chairman Richmond cosponsoring and voting for H.R. 1 when it passed the House in March 2019, and we continue to strongly urge Senator McConnell to bring it up for a vote in the Senate.

H.R. 4, the John Lewis Voting Rights Advancement Act.—Before elections officials close, move, or consolidate polling locations or make other changes to voting procedures, covered jurisdictions with a history of discrimination would need sign-off from the Department of Justice to ensure that these changes aren't being made for discriminatory purposes. Five previous Voting Rights Act reauthorizations were signed into law by Republican presidents, most recently by President George W. Bush in 2006. As we approach the 55th anniversary of the Voting Rights Act later this week, I can't think of a better way to honor the life of Congressman John Lewis by having the Senate follow the House's lead and pass the John Lewis Voting Rights Advancement Act.

CONCLUSION

Voters should not be forced to choose between their health and their right to vote. With the 2020 election less than 3 months away, we need Congress to act now to help protect our elections so all voters can have their voices heard and votes counted. In order to ensure the 2020 elections are safe, secure, accessible, and fair, Congress must make modest investments so States and localities can implement critical voting system changes that this pandemic demands of us. At a bare minimum, we urge Senate Republicans to listen to the hundreds of thousands of Americans who have contacted their offices to urge them to support additional election funding.

And if there's a more reform-minded Senate and administration next year, Congress must pass critical reforms like H.R. 1 and H.R. 4. As President Obama made plain just last week, the fight for a more just and responsive democracy demands we continue the march of John Lewis. We must ensure all voices can be heard in our democracy by restoring voting rights, enacting automatic voter registration, and ending partisan gerrymandering, as H.R. 1 and H.R. 4 would do. And if Republicans refuse, we must cast aside the filibuster as the "Jim Crow relic" it represents. Thank you.

Mr. RICHMOND. Thank you, Ms. Albert, for your testimony.

I now recognize Ms. McReynolds to summarize her statement for 5 minutes.

STATEMENT OF AMBER MC REYNOLDS, CHIEF EXECUTIVE OFFICER, NATIONAL VOTE AT HOME INSTITUTE

Ms. MCREYNOLDS. Thank you, Mr. Chairman, Members, and staff. Thank you for inviting me to provide testimony about the resiliency and readiness of our election systems during this unprecedented public health crisis.

The pandemic has appended all aspects of our lives, and the voting process is no different. Simply put, our democracy is essential, and we must do everything we can to ensure our election system is ready, resilient, and secure. Let me be very clear: Election officials are working each and every day to make this happen, even in extraordinary and extremely challenging circumstances, and often with one hand tied behind their backs, due to outdated laws and a lack of funding and resources.

Extraordinarily long lines or other challenging circumstances that voters often face, even prior to this year, are usually the most visible symptoms of a policy or resource problem.

Election officials have responded to difficult circumstances with little support, and will attempt to do so again this year, but this year is unprecedented. They need support from elected leaders that have the power to help. They are on the front lines delivering democracy to all voters in small towns and metro areas across the United States. It is only right that policy makers, not only at the

Federal level, but also at the State level, respond to their needs. Extraordinary challenges call for extraordinary solutions.

What is clear to me during this pandemic and other challenges we have faced as a Nation is that Americans are resilient, and we need a voting process that is proven, resilient from a pandemic, from unfairness, from barriers, from foreign adversaries, from administrative deficiencies, and from outdated policies that create challenges. We need a system that can withstand all of those issues.

The fact is the pandemic has exposed challenges in most States historical reliances on in-person voting on one single day that requires a large number of people and resources to manage. In too many primary States this year, the closure of polling places, poll worker shortages, long lines, insufficient training, and voters' reluctance to enter crowded environments, along with surges, unprecedented surges in absentee ballot requests that went unfilled due to the administrative burdens to process, left many voters unable to safely exercise their fundamental right to vote.

It is our elected leaders' responsibility to ensure that our democracy functions, and that all voters have access to participate. Enabling voting-at-home options is one way to solve the challenges election officials, and by extension, voters, face during this pandemic. Voting-by-mail is proven, time-tested, and secure, and it dates all the way back to the Civil War.

The mail ballot model, as designed, puts voters first, and has proven to be resilient during both natural disasters and the current pandemic. It is possible to improve to improve the voting experience, streamline administrative processes, enhance security, all while conserving valuable resources, increasing turnout, and increasing trust in Government. Voters have been voting this way at home, safely and securely for decades, in many States. From Utah to Colorado, California, Oregon, Washington, now Washington, DC, Vermont, and now Nevada, after this weekend, policy makers have acted to ensure voters have a clear range of options to vote safely and securely, because no one should have to choose between voting and protecting their health.

What does this process look like? In the 8 States plus District of Columbia, as of August of this year, just recently Nevada passed, voters will be mailed a ballot in advance of the election and have multiple options to return that ballot.

In the rest of the States, voters can request a ballot to be mailed to them. A small number of those States still require an excuse to be provided with the ballot request, and even fewer still limit options based on the voter's age.

But every single State offers an option to vote at home. Whether you call it absentee, vote-by-mail, mail-in ballots, it means that a ballot is being sent to the voter by mail, the voter completes the ballot, and the ballot is returned. This method of voting has been proven to be safe and secure, and it includes strong safety measures to ensure the authenticity of the ballots, and in some States, this includes ballot tracking from the day the ballots are mailed all the way through when they are processed.

Now, as a couple of notable considerations, and as you mentioned the CISA report, the CISA report that was released on Friday that

talked about the importance of securing vote-by-mail systems noted that disinformation risks to mail-in voting infrastructure and processes is similar to that of in-person voting while utilizing different content. Threat actors may leverage limited understanding regarding mail-in voting to mislead and confuse the public. This includes casting doubt without evidence about the mail ballot process, thus combating disinformation and misinformation is a critical aspect of election officials' work to secure the election. Expanding vote-at-home options is nonpartisan and supported by leaders on both sides of the aisle.

A second notable consideration is the recent changes to the USPS processes and delivery time lines that will have a significant impact on our election process, regardless of the voting method. Mail ballots are just one piece of how the Post Office supports election infrastructure. Federal and State laws have legal mandates with regards to sending voter registration information, ballot issue notices, election information, poll worker appointment letters, polling place notification cards, signature cards, address update notifications, and other required mailings.

All of these legally required mailings are at risk if the Post Office is not able to process mail effectively, or experiences delays.

Some States have also not updated their laws with regards to processing, ensuring adequate time to process ballots. These States include Michigan, Pennsylvania, Wisconsin, New York, Maryland, and Alabama, and others. This is exactly why we have seen delays in election results because election officials don't have adequate time to process ballots in advance of Election Day.

As with every part of our election system, we must be able to deter, detect, and hold accountable any bad actor who tries to interfere with our election process.

While voter fraud is exceedingly rare in elections regardless of voting method, it is critical for election officials to detect malicious activity, and for voters to report suspicious activity to the appropriate authorities.

Our democracy functions when every eligible voter is able to exercise their right to vote. Voters have already chosen to vote at home in record numbers in the primaries, and they will continue to do so.

Our democracy is essential, and we need to be sure that our systems are secure from any interference and any misinformation and disinformation as noted in the CISA report on Friday.

No election system is perfect, and this is why it is critical to continually review and improve systems by enhancing security access transparency, particularly in this unprecedented time. An example of the necessary improvement is the implementation ballot tracking system that many States are working on right now. Another example is advanced auditing techniques, such as risk-limiting audits. We cannot settle for when this moment and this unprecedented crisis calls us to do better.

Democracy is the shared DNA of our Nation, to our people, to our communities. We must do everything we can to ensure that the elections are secure. Going into November, election administration must be about who votes, not who wins. You have the authority to create a path for the American people and for the American Demo-

cratic method that voters of all stripes can be confident in. Let's do that together. Thank you.

[The prepared statement of Ms. McReynolds follows:]

PREPARED STATEMENT OF AMBER MCREYNOLDS

AUGUST 4, 2020

Chairman, Members & staff, thank you for inviting me to provide testimony about the resiliency and readiness of our election systems during this unprecedented public health crisis.

The pandemic has upended all aspects of our lives and the voting process is no different. Simply put, our democracy is essential and we must do everything we can to ensure our election system is ready, resilient, and secure. Let me be clear: Election officials are working each and every day to make this happen, even in extremely challenging circumstances and often with one hand tied behind their backs due to outdated laws and a lack of funding and resources. Extraordinarily long lines or other challenging circumstances that voters often face are usually the most visible symptoms of a policy or a resource issue. Election officials have responded to difficult circumstances with little support and will attempt to do so again this year. But this year is unprecedented. They need support from elected leaders that have power to help. They are on the front lines, delivering democracy to all voters in small towns and in metro areas, and it is only right that policy makers respond to their needs. Extraordinary challenges call for extraordinary solutions.

What is clear to me during this pandemic and other challenges we have faced as a Nation is that Americans are resilient, and we need a voting process that is proven—resilient from a pandemic, from unfairness, from barriers, from foreign adversaries, from administrative deficiencies, and from outdated policies that create challenges. We need a system that can withstand all.

The fact is the pandemic has exposed challenges in most States' historical reliances on in-person voting on one single day that require a large number of people and resources to manage. In too many primary States this year, the closure of polling places, poll worker shortages, long lines, insufficient training, and voters' reluctance to enter crowded environments threaten the ability to vote in-person, and surges in absentee ballot requests that went unfulfilled left many voters unable to safely exercise their fundamental right to vote. It is our elected leaders' responsibility to ensure our democracy functions and all voters have access to participate. Enabling voting at home options is one way to solve the challenges election officials and by extension, voters face during this pandemic. Voting-by-mail is proven, time-tested, and secure, and it dates back to the Civil War.

The mail ballot model puts voters first and has proven to be resilient during both natural disasters and the current pandemic. It is possible to improve the voting experience, streamline the administrative process, enhance security, all while conserving valuable resources, increasing turnout, and increasing trust in Government. Voters have been voting this way at home safely and securely for decades in many States. From Utah, to Colorado, California, Oregon, Washington, DC, Vermont, and now Nevada, policy makers have acted to ensure voters have a clear range of options to vote safely and securely. No one should have to choose between voting and protecting their health.

What does the process look like?

1. In 8 States plus DC (CA, CO, DC, HI, NV, OR, UT, VT, and WA, all as of August 2020) voters will be mailed a ballot in advance of the election and have multiple options to return their ballot at a secure drop box, voting location, or by mailing the ballot back through the postal service.

In the rest of the States, voters can request that a ballot be mailed to them. A small number of those States still require an excuse to be provided with the ballot request, and even fewer still limit options based on a voter's age.

Every State offers an option to vote from home. Whether you call it absentee, vote-by-mail, mail-in ballots—it means that a ballot is being sent to the voter by mail, the voter completes the ballot, and the ballot is returned.

2. Voting at home is a safe and secure method of voting and the process includes strong security measures that ensure the authenticity of ballots. In some States, the process includes tracking ballots from the day they are printed to the day they are processed. Just like tracking a package ordered on-line.

3. Accurate voter information is key, which requires that election officials have the latest address information for each voter. Most States share information on voter movement across State lines, others directly contact voters based on mail

forwarding designations, death records, motor vehicle registrations, and more to make sure voter information is accurate.

4. Your ballot is as unique as you are: Every voter gets a ballot with barcodes on the envelope that correspond to the individual voter and the voter's address. The ballot itself has a removable stub, the information for the specific election, precinct style, and other variables depending on the State.

5. Once ballots are dropped off, they go through a verification process: During the process, election officials make sure that the voting record of each voter is marked and that the ballot envelope is verified before the ballot is counted, much like when a voter checks in at their polling location.

6. The ballot is then extracted from the envelope. The extraction process protects voter privacy, while maintaining the voter's identity in the barcoding process for security. Audits are conducted at each step and these audits ensure that every eligible vote received in the designated time frame is counted.

7. Then the ballots are sent to the counting room and at this point, state-of-the-art scanning equipment counts each batch of ballots. Voter intent issues on ballots (such as stray marks) are flagged for review and resolved by election officials.

8. Signature verification is a best practice security measure when combined with appropriate processes: Voters sign their ballot the same way they sign other legal documents, and that signature is verified against other official signatures on record. When done according to best practices like demographically blind review, signature verification is an important security measure that leads to greater election confidence. Also voters with signature issues are given the opportunity to "cure" their ballots, meaning that they are able to directly verify the authenticity of their ballot.

Notable considerations:

1. As noted in the CISA Report released on Friday, "Disinformation risk to mail-in voting infrastructure and processes is similar to that of in-person voting while utilizing different content. Threat actors may leverage limited understanding regarding mail-in voting to mislead and confuse the public."

   a. This includes casting doubt without evidence about the mail ballot process.

Thus, combatting disinformation and misinformation is a critical aspect of election officials' work. Expanding vote-at-home options is nonpartisan and supported by leaders on both sides of the aisle.

2. Changes to USPS processes and delivery time lines will have a significant impact on our election process, regardless of voting method. Mail ballots are just one piece of how the USPS supports election infrastructure. Federal and State laws have legal mandates with regards to sending voter registration information, ballot issue notices, election information, poll worker appointment letters, polling place notification cards, signature cards, address update notifications, and other required mailings. All of these legally required mailings are at risk if the post office is not able to process mail effectively or experiences delays.

3. Some States, such as MI, PA, WI, NY, MD, and AL, have not updated certain election laws and processes to ensure adequate time to process mail ballots, hence recent delays with election results. Local election officials have repeatedly highlighted this gap, and policy makers have not made these necessary adjustments even though they are simply operational, and not partisan. States still have time to close these holes, and support election officials.

4. As with every part of our election system, we must be able to detect, deter, and hold accountable any bad actor who tries to interfere with the election process or with an individual voter. While voter fraud is exceedingly rare in elections regardless of voting method, it is still critical for election officials to detect malicious activity and for voters to report suspicious activity to appropriate authorities.

Our democracy functions well when every eligible voter is able to exercise their right to vote.

Voters have already chosen to vote at home in record numbers in the primaries. Recent surveys show that an extraordinary number of voters are choosing to vote from home this November as well. Voters—the customers of our democracy—are sending a very clear message about how they want to vote; policy makers must respond to the needs of election officials to ensure they have the resources to serve voters effectively.

No election system is perfect, and this is why it is critical to continually review and improve systems by enhancing security, access, and transparency, particularly in this unprecedented time. An example of a necessary improvement is the implementation of ballot tracking systems that provide accountability to voters about the

status of their ballot and give election officials an ability to track ballots through the process. Another example is advanced auditing techniques such as risk-limiting audits. We cannot settle when the moment calls for us to do better.

Democracy is the shared DNA of our Nation, to our people, to our communities. We must do everything we can to ensure that it works for all, even in this most trying time. Going into November, election administration must be about who votes, not who wins. You all have the opportunity to create a path forward for the American people, and for an American democratic method that voters of all stripes can be confident in. Let's do that together.

Mr. RICHMOND. Thank you for your testimony.

Finally, I recognize Mr. Gilligan to summarize his statement for 5 minutes.

STATEMENT OF JOHN M. GILLIGAN, PRESIDENT AND CHIEF EXECUTIVE OFFICER, CENTER FOR INTERNET SECURITY, INC.

Mr. GILLIGAN. Chairman Richmond, Ranking Member Katko, and Members of the subcommittee, thank you for the invitation to appear before this important committee.

My name is John Gilligan. I am the chief executive officer of a nonprofit Center for Internet Security, or CIS. For the past 10 years, CIS has had the privilege of operating the monthly State Information Sharing and Analysis Center, the cyber threat and best practice sharing organization consists of nearly 10,000 State, local, Tribal, and territorial government organizations.

In 2018, CISA was asked to establish a parallel organization focused on U.S. election organizations. The Elections Infrastructure Information Sharing and Analysis Center or EI–ISAC is now fully operational, and has more than 2,600 State and local organizations as members. Today, I will share my views about the progress that has been made in protecting our Nation's elections' infrastructure from cyber threats.

In the summer of 2016 and into 2017, many elections' jurisdictions had immature technology security capabilities, limited cybersecurity awareness and education, and insufficient collaboration among key stakeholders at the Federal, State, and local levels. In early 2018, DHS, the Elections Assistance Commission, or EAC and the State and local elections officials came together to jointly take on a series of actions to improve the security of our elections' infrastructure. Information of the EI–ISAC was one of these actions.

In addition to the cybersecurity activities that State and local election officials undertake on their own, today the technical protections deployed across the elections' infrastructure have significantly improved since 2018. I will highlight 3 of these technologies, comprising a layered, cyber-defense approach, each funded, at least in part, to Congressional appropriation.

First is the deployment of the Albert Network Monitoring sensors at every State-level elections organization and a total of 270 Albert Network Monitoring devices deployed to local elections offices.

Second, an endpoint detection and response program with the deployment of cyber sensors for individual systems in the elections infrastructure. Thousands of these sensors are being deployed as we speak.

Third, a capability called malicious domain blocking and reporting that prevents elections offices' computers from connecting to known malicious sites.

In the area of cyber awareness and education, a set of broad initiatives has enhanced elections officials' understanding of cyber attacks and what they should do to assess their organization's cyber readiness. Conferences, webinars, tabletop exercises, State-sponsored cyber education events, educational materials, and situational updates from EI–ISAC, as well as on-line courses sponsored by DHS's CISA organization, the EAC, and third-party organizations, have resulted in a dramatic improvement in the cybersecurity awareness of elections official.

In addition to Federally-funded activities, CIS continues to invest our own funds and seeks private grant support to develop best practice guidance and tools for elections officials.

While elections officials are not cybersecurity experts, they now better understand the nature of cyber threats, the available technical solutions, and what to do in response to a cyber event.

Finally, with regard to the critical area of collaboration, the working relationships and partnerships among Federal, State, and local organizations have shown a remarkable maturation. CISA, the EI–ISAC, associations representing the secretaries of state or NASS, State elections directors, or NASED, local elections officials, IGO, the EAC and the elections center, as well as elections vendors and other private and public organizations have been working collaboratively with elections offices for the past several years to improve the office's cybersecurity posture, and relationships continue to improve.

Simply put, compared to 2016 and 2018, the security of the election's infrastructure looks quite different in 2020. While there are no guarantees on cybersecurity, I can assure you that the security defenses that we have in place for November 2020 are vastly improved over those in place a short 4 years ago.

Congress, the elections officials, CISA, and a host of public and private organizations, should be rightfully proud of the progress that has been made in this area.

I close by respectfully recommending that Congress continue to emphasize the importance of collaboration and cyber technology innovation. I also encourage you to focus on the attention on this and disinformation in American elections, major vulnerability through November, and beyond.

In this last period, CIS has developed a misinformation reporting portal for elections officials in order to simplify reporting of elections-related lists and disinformation. We piloted the system with elections officials in 5 States, and have engaged with DHS, NASS, NASED to promote this capability to social media platform. We believe that this capability will be a valuable tool of increasing visibility of elections-related mis- and disinformation. This concludes my oral remarks, I look forward to your questions.

[The prepared statement of Mr. Gilligan follows:]

PREPARED STATEMENT OF JOHN M. GILLIGAN

AUGUST 4, 2020

Chairman Richmond, Ranking Member Katko, and Members of the subcommittee, thank you for inviting me today to this hearing. My name is John Gilligan, and I serve as the president and chief executive officer of the nonprofit Center for Internet Security, Inc. (CIS). I have spent most of my career in service to the Federal Government, including serving as the chief information officer of both the U.S. Department of Energy, and the U.S. Air Force. I appreciate the opportunity today to share our thoughts on the current state of American election security. I look forward to offering our ideas on how we can collectively build on the progress being made in this important area of critical National security.

Free and fair elections are essential to our democracy. In the United States, elections are highly decentralized with more than 8,000 jurisdictions across the country responsible for the administration of elections. While the Federal Government provides some laws and regulations, the Federal Government does not administer elections and has a limited role in dictating how the process is conducted. States act as the primary authority for the laws and regulations that govern the process of conducting an election and, accordingly, States have substantial discretion on the process of conducting elections through Secretaries of State and State election directors. State and local officials have been defending our elections for over 2 centuries. The 2016 election was less about a new threat and more about the breadth and depth of threat activity. Fortunately, since 2016 we have collectively learned a great deal about how best to respond to these cyber risks and to prepare for the 2020 election.

In short, I would like to: (1) Provide you a short background about CIS; (2) describe the role and functions of the Elections Infrastructure Information Sharing and Analysis Center (EI–ISAC), which we operate in conjunction with the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) with funding from Congress; (3) describe our collaboration with elections offices and key stakeholder organizations; (4) describe CIS's other, significant best practice work in this area; and (5) respectfully make 3 recommendations.

(1) BACKGROUND ABOUT THE CENTER FOR INTERNET SECURITY

Established in 2000 as a nonprofit organization, the primary mission of CIS is to advance cybersecurity readiness and response. CIS was instrumental in establishing the first guidelines for security hardening of commercial Information Technology (IT) systems at a time when there was little on-line security leadership. Today, CIS works with the global security community using collaborative deliberation processes to define security best practices for use by Government and private-sector entities. The approximately 250 professionals at CIS provide cyber expertise in 3 main program areas: (1) The Multi-State Information Sharing and Analysis Center (MS–ISAC) and, more recently, the EI–ISAC; (2) the CIS Benchmarks; and (3) the CIS Critical Security Controls. I describe each briefly below.

The CIS Benchmarks [1].—CIS produces the largest number of authoritative, community-supported, and automatable security configuration benchmarks and guidance. The CIS Benchmarks (also known as "configuration guides" or "security checklists") provide highly-detailed security setting recommendations for a large number of commercial IT products, such as operating systems, database products and networking systems. These benchmarks are vital for any credible security program. The CIS Benchmarks are developed through a global collaborative effort of public and private-sector security experts. Over 200 consensus-based Benchmarks have been developed and are available in PDF format free to the general public on the CIS or NIST websites. An automated benchmark format along with associated tools is also available through the purchase of a membership. CIS has also created a number of security configured cloud environments, called "hardened images" that are based on the benchmarks that we are deploying in the Amazon, Google, Oracle, and Microsoft cloud environments. These hardened images help ensure that cloud users can have confidence in the security provided within the cloud environment they select. The CIS Hardened Images are used world-wide by organizations ranging from small, nonprofit businesses to Fortune 500 companies.

The CIS Benchmarks are referenced in a number of recognized security standards and control frameworks, including:

[1] Find out more information about the CIS Benchmarks here: *https://www.cisecurity.org/cis-benchmarks/*.

- NIST Guide for Security-Focused Configuration Management of Information System
- Federal Risk and Authorization Management Program (FedRAMP) System Security Plan
- DHS Continuous Diagnostic Mitigation Program
- Payment Card Industry (PCI) Data Security Standard v3.1 (PCI)
- CIS Controls
- U.S. Department of Defense Cloud Computing Security Requirements Guide.

The CIS Controls[2].—CIS is also the home of the CIS Critical Security Controls (or the CIS Controls), the set of internationally-recognized, prioritized actions that form the foundation of basic cyber hygiene and essential cyber defense. They are developed by an international community of volunteer experts and are available free on the CIS website.

The CIS Controls act as a blueprint for system and network operators to improve cyber defense by identifying specific actions to be done in a priority order—achieving the goals set out by the NIST Cybersecurity Framework (CSF). Moreover, the CIS Controls are specifically referenced in the NIST CSF as one of the tools to implement an effective cybersecurity program.[3]

To bring another level of rigor and detail to support the development and implementation of the CIS Controls, CIS leveraged the industry-endorsed ecosystem that is developing around the MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) Framework.[4] The ATT&CK Model comprehensively lists attack techniques that an attacker could use at each step of an attack. Our analysis shows that implementing the CIS Controls mitigates approximately 83 percent of all the techniques found in ATT&CK.[5] This implies that application of the CIS Controls provides significant security value again a very wide range of potential attacks, even if the details about those attacks are unknown.

MS–ISAC[6].—In late 2002, the Multi-State Information Sharing and Analysis Center (MS–ISAC) was created by the State of New York with the recognition that the State government community needed an information-sharing mechanism (i.e., an information sharing and analysis center or "ISAC") to coordinate cybersecurity efforts and promote best practices. In January 2003, the MS–ISAC had its first meeting, formally launching an ISAC for State governments. DHS first reached out to the MS–ISAC in September 2004 and began providing some funding. In 2010, DHS officially designated the MS–ISAC as the key resource for cyber threat prevention, protection, response, and recovery for the Nation's SLTT governments and issued the first Cooperative Agreement. This designation [sic] Also, in 2010, the MS–ISAC moved to its current organizational home within CIS, where it has since resided.

The members of the MS–ISAC, the largest ISAC in the world, include all 56 States and territories, and over 10,000 other SLTT government entities including local governments, schools, hospitals, and publicly-owned water, electricity, and transportation elements of the U.S. critical infrastructure. MS–ISAC's 24x7 cybersecurity operations center provides: (1) Cyber threat intelligence that enables MS–ISAC members to gain situational awareness and prevent incidents, consolidating and sharing threat intelligence information with the DHS National Cybersecurity and Communications Information Center (NCCIC); (2) early warning notifications containing specific incident and malware information that might affect them or their employees; (3) incident response support; and (4) various educational programs and other services. Furthermore, MS–ISAC provides around-the-clock network monitoring services with our Albert network monitoring devices for many SLTT networks, analyzing over 1 trillion event logs per month. Albert is a cost-effective Intrusion Detection System (IDS) that uses open source software combined with the expertise of the MS–ISAC 24×7 Security Operations Center (SOC) to provide enhanced monitoring capabilities and notifications of malicious activity. In 2019, MS–ISAC analyzed, assessed, and reported on over 72,000 instances of malicious activity for over 8,500 MS–ISAC members. CIS is installing a layered set of cyber defense capabilities for the elections infrastructure that results what is often referred to as "defense-in-depth." The Albert IDS capabilities are being complemented with end-

---

[2] Find out more information about the CIS Controls and download them for free here: *https://www.cisecurity.org/critical-controls.cfm*.

[3] *NIST Framework,* Appendix A, page 20, and throughout the Framework Core (referred to as "CCS CSC"—Council on Cyber Security (the predecessor organization to CIS for managing the Controls) Critical Security Controls).

[4] MITRE ATT&CK Framework, *https://attack.mitre.org/*.

[5] *CIS Community Defense Model* v 1.0, the Center for Internet Security, August 2020.

[6] Find out more information about the MS–ISAC here: *https://msisac.cisecurity.org/*. A list of MS–ISAC services here: *https://www.cisecurity.org/wp-content/uploads/2018/02/MS-ISAC-Services-Guide-eBook-2018-5-Jan.pdf*.

point protection capabilities, as well as automated blocking of known malicious internet sites.

(2) THE ROLE AND FUNCTIONS OF THE EI–ISAC

After the interference in the 2016 election, DHS, the National Association of Secretaries of State (NASS), the National Association of State Election Directors (NASED), the Elections Assistance Commission (EAC), as well as local elections organizations, and CIS discussed the possibility of creating an ISAC devoted solely to the Nation's elections infrastructure. In 2017, DHS agreed to conduct a pilot elections ISAC with 7 States. This pilot group developed and tested a range of products geared toward communicating cybersecurity issues to State and local election officials. Upon the success of that pilot, in 2018, DHS and the Election Infrastructure Subsector Government Coordinating Council tasked CIS to stand up the Elections Infrastructure ISAC (EI–ISAC). Leveraging the services offered and experience gained through the MS–ISAC, the EI–ISAC is now fully operational[7] with all 50 States and the District of Columbia participating, and over 2,600 total members, including the election vendor community. The EI–ISAC provides elections officials and their technical teams with regular updates on cyber threats, cyber event analysis, and cyber education materials.

Deploying More Albert Sensors.—As part of the initial launch, CIS was also tasked with deploying a network of Albert sensors to all 50 State election offices and the 5 largest counties in States that have bottom-up and hybrid voter registration processes. Since then, all 50 States have deployed and many States have leveraged HAVA funding to procure additional Albert sensors for every county election office. CIS now processes data from 269 Albert sensors monitoring State and local election networks, which support on-line elections functions such as voter registration and election night reporting. The Albert sensors processed 30 petabytes of data in the first half of 2020, resulting in nearly 2,000 cyber event notifications to elections offices.

Improving Situational Awareness.—Starting with the 2018 primaries and midterm elections, the EI–ISAC has hosted the Election Day Cyber Situational Awareness Room, an on-line collaboration forum to keep elections officials aware of cyber and non-cyber incidents and potential cyber threats for any State-wide or National election. More than 600 elections officials, Federal partners, and election vendors have participated in these forums. It is expected that participation in the situation room will likely grow to all 50 States for the November 2020 General Election.

Piloting New Technology.—Earlier this year, the EI–ISAC, in cooperation with DHS CISA and Congressional appropriators, expanded our protection of elections through 2 new programs aimed at addressing the needs of lower-resourced organizations. These new programs also provide a defense-in-depth capability where multiple cyber defense capabilities working together improve threat situational awareness and increase effectiveness in defeating malicious threats:

The Endpoint Detection and Response (EDR) Pilot for Elections Infrastructure provides a sophisticated cybersecurity technology that complements the network monitoring performed by the Albert network sensors for the elections community. The EDR sensors also expand and enrich the threat intelligence available to the MS– and EI–ISAC. The EDR solution has the capability to monitor internal network traffic, and the EDR agents can programmatically block malicious activity and quarantine compromised systems, shifting the immediate cybersecurity response effort from election offices to the CIS SOC. This will allow smaller or less mature offices to take advantage of the same protections as larger offices improving the community's cybersecurity. CIS is currently deploying EDR sensors, focusing on critical systems in the elections infrastructure, like voter registration, election management, and election night reporting.

The Malicious Domain Blocking and Reporting (MDBR) Pilot provides a commercial secure Domain Name System (DNS) service to block access from SLTT member organizations to known malicious domains. In effect, the capability prevents the execution of the majority of malicious attacks associated with ransomware, malware, command and control, and phishing domains. Anonymized data from this offering will be correlated with other threat intelligence feeds and provided in threat reporting to CISA and the broader SLTT community. The MDBR capability can be implemented in minutes and recent NSA analysis indicates that this solution can reduce the ability for 92 percent

[7] Find out more information about the EI–ISAC here: *https://www.cisecurity.org/ms-isac/*. A list of EI–ISAC services can be found here: *https://www.cisecurity.org/ei-isac/ei-isac-services/*.

of malware, from a command-and-control perspective, to deploy malware on a network.[8] CIS began deploying this capability in early July. While the capability is available to all SLTT organizations, the priority is to deploy to elections organizations prior to November.

(3) COLLABORATION WITH ELECTIONS OFFICES AND KEY STAKEHOLDER ORGANIZATIONS

Both as a part of CIS's role in operating the EI–ISAC as well as efforts not funded by the Government, we have placed emphasis on establishing a trusted relationship with elections officials and other key stakeholders. CIS has participated and conducted cyber exercise for elections offices, conducted numerous cyber webinars, and made in-person visits to almost every State and many local elections jurisdictions, many of these activities in partnership with DHS CISA. In addition, we have worked closely with other key organizations supporting the elections community such as the National Association of Secretaries of State (NASS), the National Association of State Elections Directors (NASED), the Elections Assistance Commission (EAC), the Election Center, and the International Association of Government Officials (IGO). Finally, we have also worked closely with private-sector organizations such as Harvard's Belfer Center, Microsoft, elections vendors, and other organizations who are working to improve the security of our elections infrastructure.

(4) CIS'S OTHER, SIGNIFICANT ELECTION SECURITY BEST PRACTICES

CIS also makes significant investment is Election Security Best Practices and related tools. Since the release of our *Handbook for Election Infrastructure Security* in 2018, CIS has become the leading non-Government provider of election security advice to SLTT election authorities, election technology vendors, and the elections community at large.

The *Handbook for Election Infrastructure Security* provides 88 best practices covering the entirety of the election administration technology. These best practices have been widely adopted by the election community with State and local offices in 34 States using them as a metric for assessing the security of elections systems. To assist States and local election officials assess and adopt these best practices, CIS developed and maintains the Election Infrastructure Assessment Tool (EIAT). The EIAT is a free on-line tool designed to help election officials assess their IT infrastructure against the 88 best practices from the Handbook. We have had over 600 users representing 34 States and 265 local election jurisdictions take advantage of the EIAT.

A Guide for Ensuring Security in Election Technology Procurements was released in May 2019 to assist election officials with ensuring security is properly accounted for in their election technology procurements. This guide provides 33 recommended questions to ask of election technology providers and assist election officials assess responses by providing descriptions of good and bad responses.

CIS released its *Security Best Practices for Non-Voting Election Technology* in October 2019 to address internet-connected election technology such as electronic poll books, electronic ballot delivery, and election night reporting systems. This guide covers 5 areas of technology: Network and Architecture, Servers and Workstations, Software Application, Data, and Administration. The areas were chosen carefully based on similarities in threats, mitigations, and governance.

CIS has followed up these election technology best practices with an on-going pilot project on how to verify systems against these best practices. Traditional voting systems are verified against large monolithic standards using lengthy and expensive certification campaigns. Our alternative approach, known as Rapid Architecture-Based Election Technology Verification (RABET–V), focuses on the need for internet-connected election technology to be responsive and adapt quickly to changes in the threat landscape. RABET–V is addressing this with a process model that provides assurances of security, reliability, and functionality in a risk-based, flexible, change-tolerant process. We are currently piloting this process with several election technology vendors and a steering committee consisting of the Election Assistance Commission, DHS CISA, Federal Voting Assistance Program, and the States of Wisconsin, Ohio, Maryland, Texas, Pennsylvania, and Indiana. We anticipate a report following the November General Election.

[8] "The NSA is piloting a secure DNS service for the defense industrial base", Cyberscoop, June 18, 2020, *https://www.cyberscoop.com/nsa-secure-dns-service-pilot-defense-industrial-base/*.

Misinformation Reporting Portal Pilot.[9] CIS is currently producing a better means for election officials to report election infrastructure misinformation and disinformation to the social media platforms for their investigation and adjudication. Currently, a limited set of election officials can report to Facebook and Twitter using the means provided directly by the social media platform. Elections officials must pre-register with the platform and report independently to each one. CIS is working to facilitate a single reporting portal where election officials can report the suspected misinformation and disinformation once, and have it distributed to the various social media platforms. We have been working closely with DHS, NASS, and NASED, along with 5 States to vet and promote this concept to the social media platforms.

The Misinformation Reporting Portal will provide elections officials with a single place (i.e., the portal) for reporting mis- and disinformation across multiple social media platforms with a streamlined, consistent user experience. In addition, the entire elections community will have visibility of what's going on with mis- and disinformation in the elections community within and outside their jurisdictions, including to see trends and be able to strategically respond. The portal will also streamline and standardize reporting for the social media organizations. In addition, voters will have the benefit of more rapid correction of erroneous information, leading to improved voter confidence.

(5) THREE RECOMMENDATIONS TO CONTINUE SECURING ELECTIONS

While much progress has been made over the last 4 years, we know that the threat remains, and, as a Nation, we must continue to address these new risks and vulnerabilities. We respectfully recommend 3 courses of action to keep our elections safe and secure. We must: (1) Continue to emphasize the importance of collaboration and foster collaboration across all elections stakeholders; (2) continue to innovate and leverage evolving security and applicable commercial technologies; and (3) consider how best to address the impact of mis- and disinformation on American elections.

Emphasize Collaboration.—We hear much of the importance of resilience in the homeland security context. When you look back on it, the post-2016 response to securing our elections is an excellent example of a successful public-private partnership. The recognized shortfalls in 2016 have helped highlight a National crisis that has been responded to by many organizations working together.

NASS, NASED, the Election Center, IGO and their respective members remain central in running American elections. Collectively, they continue to provide the deep expertise in exactly how the complicated function of operating elections works, and how new processes and technology can best be used in each jurisdiction. Other State and local associations like the National Governors Association (NGA), the National Conference of State Legislatures (NCSL), the National Association of State Chief Information Officers (NASCIO), the National Association of Counties (NACo), the National League of Cities (NLC), the National Emergency Management Association (NEMA), and others have stepped up and collaborated to identify and facilitate the best approaches to improving security of the elections infrastructure within their jurisdictions.

On the Federal side, Congressional appropriators were several times able to provide significant funding for critical election security grants that were, simply put, essential to help prepare elections offices with limited resources across the country. An active and engaged DHS CISA enthusiastically accepted the role of the Nation's Risk Advisor on elections, used their convening power and bully pulpit as the lead Federal agency to good effect, and CISA continues to be an excellent partner in the MS– and EI–ISACs. Despite having one of the smallest budgets in the Federal Government and new leadership, the Election Assistance Commission (EAC) efficiently distributed $825 million in grants to the States, helped develop guidance around voting as safely as possible during the COVID–19 pandemic, and stood up a RABET–V (with CIS as described above).

Further, the elections vendors, private sector, public and private universities, think tanks and foundations, as well as nonprofit corporations like CIS have come together to help address the technical, process, and educational challenges facing the U.S. elections community. The result is that the protection capabilities of our elections infrastructure are enormously improved from 2016 and even where they were in 2018. However, it is recognized that we are not yet where we want to be

[9] The RABET–V and Misinformation Reporting Portal are projects being funded by the nonprofit Democracy Fund.

and the threat continues to increase. It will take continued collaboration to sustain and hopefully even accelerate the progress that we have seen over the past 3 years.

Continue to Innovate.—As noted above, the progress made in deploying additional technical measures and in education and training since November 2016 is impressive. However, there are opportunities to improve in each area. A danger when addressing the sensitive area of elections is to be overly cautious in assessing and piloting new methods and technical solutions. CIS was grateful to be given funding from Congress and tasking from CISA to pilot EDR and the MDBR technology. We are already seeing that these technologies will be important capabilities to protect our elections infrastructure. Working with the EAC, we are piloting what we hope will be a much quicker and less costly process for verifying elections systems. We encourage Congress to continue to support experimentation and innovation so that we can continue to leverage the best talent and capabilities that the country has to offer in a way that produces the most value for the American taxpayer.

Address the impact of mis- and disinformation on elections.—While we have made great strides in improving resilience against cyber threats, perhaps the biggest challenge that we face as a Nation going forward is how we address the impact of mis- and disinformation on elections. While we treasure our rights granted to all citizens by the First Amendment, the power of social media in shaping opinions and attitudes is expanding rapidly. CIS is working to help address the challenge of identifying and reporting deliberate or accidental misinformation or disinformation that might prevent voters from exercising their right to vote. This is a first step. However, the broader challenge is to establish norms and conventions that will help voters understand what is factual and what is opinion or even deliberate attempts to mislead. We would encourage Congress to take an incremental approach to addressing this challenge.

CONCLUSION

Securing American elections is a complex, decentralized enterprise that is fundamental to preserving our democracy. Fortunately, our State secretaries of state, State elections directors, and elections officials have been successfully defending our elections for over 2 centuries. Furthermore, since 2016, we have learned much about how this new risk can be defended. CIS is proud to have developed and to operate the Elections Infrastructure ISAC (EI–ISAC), and to have devised several other significant best practices to help the with this vital task.

To that end, CIS is committed to a long-term effort to continuously advance and promote best practices for elections security as part of a National response to threats against election infrastructure.

Mr. RICHMOND. Thank you. I want to thank all the witnesses for their testimony. I see that we have been joined by the Chairman of the full committee. I will recognize the gentleman from Mississippi, Mr. Thompson, for his opening statement.

Mr. THOMPSON. Thank you very much. Thank you very much, Mr. Chairman. I appreciate the opportunity to speak. As you know, we are less than 100 days away from the election, and House Democrats are working hard to persuade Senate leadership to provide additional election assistance to help States administer safe, secure, and auditable elections during the COVID–19 pandemic. This hearing could not come at a more appropriate time.

Last week, we celebrated the life of Congressman John Lewis. As we mourned our loss, we grappled with the tremendous task of how best to honor his legacy. In his final days, Congressman Lewis committed a lifetime of fighting for justice to parting advice to guide us through this turbulent time. He challenged us to stand up for injustice. He called each of us to use our talents to build a better country than the one we inherited. We are reminded that democracy is not a state. It is an act.

This November, our Nation will participate in an election that would look like no other in our history. The COVID–19 pandemic will demand that we adopt our voting procedures to ensure that no American must choose between exercising their democratic right to

vote and protecting their health. At the same time, we must defend our democracy against adversaries who will use our differences of opinion to sow irreparable division among us.

We must remain vigilant in defending the truth and keep the public informed to deny our adversaries the opportunity to fill information vacuums with lies. Now more than ever, we each have a role to play in defending our democracy.

As Chairman of the Homeland Security Committee, I have fought to protect the voting rights of all Americans, and to secure funding to help State and local election officials replace outdated, unsecured election equipment. Last March, the House passed H.R. 1, which included the Election Security Act, which will provide funding to States to improve election security and direct a whole-of-Government response to counter foreign influence campaigns aimed at undermining confidence in our democratic institutions.

On May 15, the House passed the HEROES Act, which would provide $3.6 billion to help States navigate the challenges associated with administering November elections during COVID–19 pandemic. That is in addition to the $800 million already made available this year. Both bills are languishing in the Senate.

The recent COVID–19 relief package proposed by the Senate Majority provides no resources to help States afraid of costs of administering Federal elections. As my Senate colleagues post their tributes to Congressman Lewis, I call on them to remember the cause that was so dear to him. Access to the ballot box, and fight to include necessary voting reforms and funding to implement them in the next COVID–19 package.

Our State officials must adopt by changing outdated voting rules that prohibit no-excuse absentee voting and the early voting, both of which would release lines and crowding, making it safe to vote. The also has a role to play. They must seek out reliable sources of accurate information and engage in election process. The integrity of the November elections depend on a whole-of-Nation commitment to our democracy.

I look forward to our conversation today on that effort, and I yield back the balance of my time.

[The statement of Mr. Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

AUGUST 4, 2020

We are less than 100 days away from the election, and House Democrats are working hard to persuade Senate leadership to provide additional election assistance to help States administer safe, secure, and auditable elections during the COVID–19 pandemic. This hearing could not come at a more appropriate time.

Last week, we celebrated the life of Congressman John Lewis. As we mourned our loss, we grappled with the tremendous task of how best to honor his legacy. In his final days, Congressman Lewis committed a lifetime of fighting for justice to parting advice to guide us through this turbulent time. He challenged to us to stand up to injustice. He called on each of us to use our talents to build a better country than the one we inherited. And he reminded us that "Democracy is not a state. It's an act."

This November, our Nation will participate in an election that will look like no other in our history. The COVID–19 pandemic will demand that we adapt our voting procedures to ensure that no American must choose between exercising their democratic right to vote and protecting their health.

At the same time, we must defend our democracy against adversaries who will use our differences of opinion to sow irreparable divisions among us. We must re-

main vigilant in defending the truth and keep the public informed to deny our adversaries the opportunity to fill information vacuums with lies. Now more than ever, we each have a role to play in defending our democracy.

As Chairman of the Homeland Security Committee, I have fought to protect the voting rights of all Americans and secure funding to help State and local election officials replace outdated, unsecure election equipment. Last March, the House passed H.R. 1, which included The Election Security Act, which would provide funding to States to improve election security and direct a whole-of-Government response to counter foreign influence campaigns aimed at undermining confidence in our democratic institutions.

On May 15, the House passed the HEROES Act, which would provide $3.6 billion to help States navigate the challenges associated with administering November elections during the COVID–19 pandemic. That is in addition to the $800 million already made available this year. Both bills are languishing in the Senate.

The recent COVID–19 relief package proposed by the Senate Majority provides no resources to help States defray the costs of administering Federal elections. As my Senate colleagues post their tributes to Congressman Lewis, I call on them to remember the cause that was so dear to him—access to the ballot box—and fight to include necessary voting reforms and the funding to implement them in the next COVID–19 package.

Our State officials must adapt by changing outdated voting rules that prohibit no-excuse absentee voting and early voting, both of which would reduce lines and crowding, making it safer to vote. The public also has a role to play. They must seek out reliable sources of accurate information and engage in the election process. The integrity of the November elections depends on whole-of-Nation commitment to our democracy.

Mr. RICHMOND. Thank you, Chairman, for this opening statement.

I will remind the subcommittee that we will each have 5 minutes to question the panel. I will now recognize myself for questions. My first question will be to all witnesses.

As you know, the President and Attorney General, who I had an opportunity to question last week, have repeatedly tried to cast mail-in voting as fraudulent, illegal, or tantamount to rigging an election. On Friday, however, CISA released a mail-in voting and 2020 infrastructure risk assessment, which considered a number of risks to vote-by-mail, but ultimately found that, "All forms of voting, in this case mail-in voting, brings variety of cyber and infrastructure risks. Risk to mail-in voting can be managed through various policies, procedures, and protocols, and controls."

No. 1, what were your takeaways from the risk assessment? No. 2, is there more that CISA or other Federal agencies can be doing to promote confidence in safe, secure, mail-in voting this November? Any of you? Mr. Levine, I see that you are ready.

Mr. LEVINE. Chairman, thank you for that question. You know, in terms of the takeaways, the CISA report, I think, was a really important document. I think it really showed a blueprint, like for the kinds of things, security-wise, that folks ought to consider, right, when they are administering an election via vote-by-mail.

Facts matter. This document is littered with facts that unambiguously state that vote-by-mail is a safe and secure process. But it does also walk through, right, some really important pieces that I think are worth mentioning. No. 1, some of the factors to consider with vote-by-mail are a bit different, right? It is worth noting that, you know, in terms of doing vote-by-mail, if the voter registration database is not as accurate, your ability after the fact to go show up at a polling place and cast a ballot, right, takes on a different kind of thing than if, in fact, you are able to go to a polling place, right, on Election Day.

I think the second thing that is really worth noting, though, is that—it was pointed out in this report is also the notion that if people spread mis- and disinformation about the vote-by-mail process, if they say that the process is easily rigged, that is the kind of thing that can be easily amplified by foreign adversaries.

In my testimony, I pointed out that authoritarian actors, like Russia and Iran, have already done that.

So, you know, I think what is really important in terms of the takeaways are No. 1, people take a look at this report so that they can understand what things they need to do to make sure they can utilize vote-by-mail in as a successful manner as possible. No. 2, I think they need to make sure, right, that they understand how that vote-by-mail process works so that they can be disseminating information to the public about how that needs to be done.

In terms of Federal authorities, you know, I think one of the things that they can be—continue to do, which they have already done, is they were reaching out in an affirmative manner, to State and local election officials as well as to civil society organizations to talk them through, right, how they can best communicate with the American public about how the vote-by-mail process can be done so that voters can have confidence, that even though voting will be different in November than previously, it is still going to be a safe and secure process.

Mr. RICHMOND. Anybody else want to join in on that answer? Ms. Albert. Mr. Gilligan.

Ms. MCREYNOLDS. Sure. Thank you, Mr. Chairman. So as I am—as previously stated, I was an elections official in Colorado, ran elections for 13 years, ran 3 different Presidential elections, along with many others, and also, transitioned various systems as—from in-person polling places, to early voting, to vote centers, to the system in Colorado.

The fact is, there is not a single State that is all vote-by-mail, or universal vote-by-mail, even though those terms get used a lot. The States that do this mail-in ballot and still preserve in-person voting options, should voters want to do that. So you really have all choices on the table.

But I was struck in the CISA report that came out, I think it included many of the best practices that my organization has recommended, but also that many States have actually adopted in recent years with regards to the vote-by-mail program. I—what struck me in the CISA guidance also was the highlight for disinformation and misinformation as being a critical risk to our elections systems. That it goes—that is true for in-person voting, it is true for early voting, and it is true for the vote-by-mail program.

So whatever we can do to combat that is critically important. We have to boost and make sure our election officials and our official State websites and local websites have and contain the best information so that voters know what to do.

But one other security risk, or actually 2 other security risks that I want to highlight is postal operations. I mentioned this in my testimony. I think it absolutely is a critical factor here. It is critical infrastructure to not only the vote-by-mail program, but elections overall, especially given all of the notices required, legal notices

that are not only at the Federal level, but also at the State level in terms of making the election run, not just mail ballots, but voter notifications, ballot-issued notices, polling place notices, all of those pieces of mail that go out through the infrastructure that is literally the only entity that serves every single customer and citizen daily, along with every election office.

The United States Post Office is literally the only entity that provides that kind of service to every American and every election office daily. We need it to be operating at full capacity. We need it to be doing what it is capable of doing to support our elections, not just mail voting, but every aspect of our election process that relies on the Post Office to do it.

The final piece, I would say, is that after administering elections for as long as I did, I would encourage everyone to rely on experts that have actually run these election processes, know where the vulnerabilities are, know how to fix those vulnerabilities, know how to address issues. There is a reason best practices have been developed over time in various States that have done this well. We didn't have that 10 years ago. We didn't have many examples of States where this procedure has operated at a very good level, has—many of those States, including Colorado where I am from, was deemed the safest place to vote in the country a couple of years ago by the Homeland Security Secretary. That is an important and critical aspect of all the different steps we did to make our system secure and make it work properly.

The one final thing I would say is I also believe it is a security risk when people can't access the voting process. If you show up, and there is a 5-hour line, or your mail ballot doesn't come to you, or you face other barriers or challenges, that is also a security problem with the election infrastructure.

So we really need to be focused on building our processes this year, and responding to all of those critical factors that prevent or inhibit the voting process from being fair for everyone.

Mr. RICHMOND. Thank you. I will—I will yield back.

I will now recognize the gentleman from Pennsylvania, Mr. Joyce, for 5 minutes.

Mr. JOYCE. Thank you very much, Mr. Richmond, for holding this hearing. There could not be a more important time as we face election 2020 in the midst of the pandemic.

I think that there are many questions, but, Mr. Gilligan, I am going to start with you. Do you feel that election officials are receiving enough information from their election system vendors about the vulnerabilities in their systems so that they can make sound purchase and maintenance decisions?

Mr. GILLIGAN. Thank you, Congressman Joyce, for the question. I think the elections officials are getting more information today than they have in the past about what are potential vulnerabilities. The—I think in years past, the election vendors didn't spend as much energy on looking at the types of cyber threats that we now know exist. So, there has been a significant sea change within the election vendors. The dilemma is, as you well know, is that many of the elections components are years old. So, there has been increased dialog between the elections vendors and the elections offices. There have been independent assessments of the elections in-

frastructure components to determine what vulnerabilities exist, and that has resulted in some improvements in the software and the capabilities of the deployed election systems. Then, I think, finally, the newer elections infrastructure components tend to be ones that have more better defenses against cyber threats.

Mr. JOYCE. Do you find that individual States are actually reaching out and increasing those protective mechanisms, particularly helping their election systems to set up the firewalls that are necessary to decrease those vulnerabilities?

Mr. GILLIGAN. Yes. So—thank you. The previous question focused on what the relationship between the elections vendors and the elections offices. What I—what I would say is there has probably been a lot more progress in the area that your current question addresses, which is the elections offices themselves. The contractor supporting them, many elections offices have gone through a cyber-navigator-type concept where they, either internally or externally, have hired individuals to come in and not only do a training, but also to do assessments of the elections' infrastructure components. CIS has actually produced some guidebooks and some tools in this area.

So that is an area that, I think, we have seen in many States that there has been a very concerted effort, there has been an effort to assess, and then to fix.

So, for example, two-factor authentication, which was not something that was popular in place in years past, is now increasingly in place. Now, what that does is it makes it far more difficult for a cyber threat actor to be able to gain access to an elections component. Redesigning of systems—you mentioned firewalls—redesigning of systems to strengthen things like firewalls, to put virtual barriers, to go into virtualization that puts barriers between the elections components, and other elements that might be on the network.

So all of these types of improvements, there has been, in my assessment, a fairly dramatic shift and resulting in, I think, a much more resilient elections infrastructure.

Mr. JOYCE. I share that enthusiasm. I think there has been a shift. But let's look at it conversely. What is the worst-case scenario, in your mind, that can occur?

Mr. GILLIGAN. Well, I actually think that, to some extent, we saw the worst-case scenario in 2016. Let me explain what I mean by that. I think the actual vote capture and vote tally systems, which is where the actual vote is captured, and then it is—is counted, those systems tend to be highly resilient, and they are not easily accessible. You almost have to get physical access to them, which makes the threat—to execute the threat fairly difficult.

The other elements, many other elements of the elections infrastructure are accessible through the network and, therefore, they share the types of vulnerabilities that we see in all network-connected systems.

So back to 2016, the—I recall, vividly, discussions with elections officials in the aftermath of 2016, and their question and comment was, Wait a minute, no votes were changed. In their mind, that was their objective is to ensure that the vote was cast, and was, in fact, counted properly. That as we all know, it wasn't just that

the vote was cast and counted properly, it is what is the confidence level that the American public has in the system? Therefore, a—an attack against the voter registration system, which did not result in anyone not being able to vote or any, you know, changes to votes, became a symbol to our American public that there is something going on here and, therefore, I am losing confidence.

So I think—I believe that the biggest challenge that we continue to have into 2020 is to—and I think some of the other speakers commented on it—is to be able to ensure that the American public has clear information about what is being done to protect the system, and if there is any particular event, to be able to very clearly identify what is the impact? That there have been lots of procedures put in place that if there is a small glitch, that that will not impact the counting of the vote or their ability to cast a vote.

Mr. JOYCE. Thank you very much for your answer. Chairman Richmond, thank you, again, for holding this important hearing today. My time has expired. I yield.

Mr. RICHMOND. The gentleman from Pennsylvania has yielded back.

I now recognize the Chairman of the full committee, the gentleman from Mississippi, Mr. Thompson.

Mr. THOMPSON. Well, I am glad to see that our witnesses have pretty much put forth the confidence in our current system.

I don't know any system that can't be improved upon. But, by and large, the Democrats on this committee have supported more funding. We have offered additional funding to secretaries of state. We have coordinated our comments with the National secretaries of state organizations and others. Because this is how we choose our leaders. Our system of democracy affords individuals the right to choose.

The State of Michigan, for instance, sent out mail applications for absentee ballots to every registered voter. That was a decision the State of Michigan made. But it is, as you said, it is an individual State's prerogative to do the process that they think works best. There is no real cookie-cutter approach. So we recognize the funding.

One of the things that I am concerned about is all of what we do for November, given the COVID–19 environment, is predicated on our Postal Service being functional.

So, Ms. McReynolds, postal workers and election officials have raised concern that changes in the Postal Service's standards could jeopardize the timely delivery of ballots. Are you concerned that changes in these standards could result in voters being disenfranchised? How should State and local election officials coordinate with the Postal Service to ensure vote-by-mail deadlines align with Postal Service standards?

Ms. MCREYNOLDS. Yes, Mr. Chairman. Thank you for the question.

I am concerned about the changes that the postal system has made recently. Coordination between election officials and the post office is absolutely critical before every single election.

As you pointed out, every system can improve. There is not a single perfect government system or government entity that exists. So there are opportunities to improve.

I have made various suggestions, frankly, from being an election official, but also being from a State where we implemented a system of mail-in ballots to every elector. So that coordination with the post office was critical.

During that time, as an election official, I not only learned about the post office, but spent time digging into their processes, their procedures, their time lines, everything about it that impacted elections. With my understanding of how all of that works, the post office is absolutely critical to the conduct, the running, and the successful conduct of elections in this country.

As I mentioned, it is not just mail ballots. It is all of the other legally-required notices—ballot issue notices, polling place notices, poll worker appointment letters, candidate notices. Official certified mail is usually how candidates are deemed to be certified on the ballot. So there are just critical elements to this.

One of the suggestions that, if you look at sort-of how the post office has operated, how it has supported elections overall, one thing that a lot of people miss is that right now, for military and overseas ballots, postage is paid for outbound and inbound ballots in every single State for every single military and overseas voter that engages with the election process.

So there is a Federal indicia right on those military and overseas ballots that that payment happens through the Department of Defense to the post office.

I have suggested a similar type of model for domestic voters because it would actually streamline a lot of the processes. The post office wouldn't have to accept payments from 7,000 or 8,000 different local election offices. It would actually be much more efficient if we had a Federal process and indicia for mail ballot postage to be paid on the outbound process and the inbound process.

So that is just one example of an administrative efficiency that I think would not only enhance service, but also streamline operations for both sides of things, election officials as well as the post office.

So those are a couple of things, and I am happy to answer more questions.

Mr. THOMPSON. Well, thank you. My time has expired.

But, Mr. Chairman, I want to highlight that any tampering with the current system puts the process at risk. There is no question we can improve it. But because we are about 90 days away from an election, it is absolutely critical that we make the current system work. Any finagling with that system puts the process in jeopardy, and I want to keep the confidence factor where it is.

With that, Mr. Chairman, I yield back. Thank you.

Mr. RICHMOND. The gentleman from Mississippi yields back.

I now recognize the gentlelady from Texas, Ms. Sheila Jackson Lee, for 5 minutes.

Well, I will now—we will get to Ms. Jackson Lee when she comes back. I will now recognize the gentleman from Rhode Island, Mr. Jim Langevin.

Mr. LANGEVIN. Thank you. Thank you, Mr. Chairman.

Ms. JACKSON LEE. Oh, I am here.

Mr. LANGEVIN. Oh, Sheila is there. Should I yield to her?

Mr. RICHMOND. Continue.

Mr. LANGEVIN. OK. Thank you, Mr. Chairman.

I want to thank our witnesses for their testimony today. Very helpful insights into your views on election security and being able to conduct successful elections this November.

Obviously, this is a cornerstone of our democracy and we want to make sure that our elections are both accessible, free, and secure, and your insights are very helpful.

The Cyberspace Solarium Commission also made several strong recommendations regarding media literacy and civics education and ways to build resiliency to disinformation campaigns.

We have seen some nascent efforts at the Federal level. For instance, CISA's principle, CISA's, they call it, pineapple pizza campaign. But the commissioners believe that much more needs to be done, that some level of dis- or misinformation is inevitable, given our commitment as a society to free speech.

Do you agree with this assessment?

Also, the Solarium Commission recommends that civics media literacy education needs to be spread out across a lifetime. It can't be a single class one takes in high school. We emphasize, for instance, the need to help seniors better understand the changing media landscape.

Do you agree with this assessment? How should we think about voter resilience as a part of our broader election security strategy? For any of the witnesses that want to start.

Mr. GILLIGAN. So, Congressman Langevin, this is John Gilligan.

Although my focus and my organization's focus is on cybersecurity, I would echo the remarks that you made and endorse the recommendations made by the Solarium Commission.

My assessment is, when I look at the risks that we have to the voting process, today I think that the potential of mis- and disinformation having an impact on the voting is greater in many regards than the potential of cyber threats.

So I think the approach that is recommended by the Solarium Commission, in part, to improve awareness among the public of mis- and disinformation, to help, especially our youth, begin to understand how to look at social media and how to look at multiple sources of information, I think is particularly important.

I believe that this issue, as I mentioned in my testimony, will be an area that will require some Congressional focus in the future, because we don't have the norms and the legislative rules that I think would be helpful going forward.

Mr. LANGEVIN. Thank you.

We have largely been talking about the November election, but the Solarium Commission's work was not necessarily specific to this year's contest as well. Indeed, we should be thinking about now the longer-term challenges, in addition to the short-term.

Can you talk about what concerns should the EAC be preparing for now to safeguard elections beyond 2020? For any of our witnesses.

Ms. MCREYNOLDS. Sure, I can jump in there. I agree with endorsing that commission's report. I think civics and disinformation, security, all of these things are really going to be life-long things that we are going have to adjust and learn to.

I am actually a single mom of two. When my ballot comes every election, it is a civics lesson for my 7- and 9-year-old, and they understand very clearly how to find good information about the voting process and we walk through that every single time.

I think in terms of the EAC, again, this is going to be a—it is a continuum of improvements over time, and we are going to have threats that we face this year that are going to be different than next year.

But this misinformation and disinformation has been plaguing the election system for the past few years and we haven't come up with a very good solution.

So I think civics education, educating voters about how to find good information and how to find trusted sources of information, is going to be absolutely critical. Then continually improving how we identify that, how we create systems that can flag those issues so that voters can clearly get the information that they need.

Mr. LANGEVIN. Thank you.

Mr. Levine, beyond the 2020 elections, any thoughts about what the EAC should be focused on?

Mr. LEVINE. Sure, Congressman, yes. To Ms. McReynolds and Mr. Gilligan's point, I think the Solarium Commission's remarks and recommendations with regards to civic education is a critical piece.

I think there are a few things that are worth noting. No. 1, we know that there are other countries that have done this in some respects better than we have. We can look to countries like Sweden and the Netherlands who also have been dealing with sort-of foreign interference threats for some time, who have more comprehensive approaches to deal with some of the threats that are outlined in terms of mis- and disinformation.

I would also underscore, to your point as well, that the Election Assistance Commission recently got some additional funding which paralleled or went in concert nicely with the Commission's recommendation and that you are seeing the EAC begin to ramp up in terms of some of the hires that they have brought on. They now have more people with a cyber background.

So I think there is a real opportunity for them to be able to step up and continue to provide cyber resources that enable State and local election officials to prepare for those evolving threats.

So I think, to your point, being able to bring people on who can assist State and local election officials who are always strapped is important. I think being able to look outward for best practices from other States who are doing this kind of work, as well as other countries, is also really important as well.

Mr. LANGEVIN. Thank you.

I know my time has expired. I just want to thank all of our witnesses for your testimony. I didn't have time to get to what we need to do to protect people with disabilities and ensuring barriers are brought down for them, but perhaps we can submit those questions for the record. But thank you for your testimony.

Mr. Chairman, thank you for holding this hearing. It is very important as we get ready for the 2020 election and beyond. Thank you for your leadership.

Mr. Chairman, I yield back.

Mr. RICHMOND. Thank you.

The gentleman from Rhode Island yields back.

I now recognize the gentlelady from Texas, Ms. Sheila Jackson Lee.

Ms. JACKSON LEE. Thank you, Mr. Chairman, and thank you to the Ranking Member, for this important hearing.

We know that *The New York Times* said that John Lewis risked his life for justice. In his op-ed he indicated that the vote is precious, but we will lose it if we do not use it.

The Constitution also acknowledges that local elections and State elections are that of those jurisdictions, but it does not deny Congress the right to involve itself by law or regulation, which I believe is extremely important in the process of which we are dealing with at this moment.

It is important to give confidence to the American people so that misinformation and disinformation and voter suppression will not keep the majority of Americans, all of Americans, from the right to vote.

So I pose this question first to our witnesses, please. Over the last couple of days there have been statements about the election should be moved. I believe there is no law and no right to move the November election, no Constitutional right to move that election. But that has been in the public atmosphere.

So I raise the question, in your professional opinions, how does the current President's persistent rhetoric about increased fraudulent ballots and changing the date of the elections—and, by the way, two Federal elections were held during the Civil War—how would that impact voter confidence?

I would raise that question with Ms. Sylvia Albert to answer that question.

Ms. ALBERT. Well, thank you for the question, Congresswoman Jackson Lee.

We have seen already that the President's rhetoric is affecting the confidence that voters have both in vote-by-mail, particularly, and also in elections in general.

I think we can be buoyed by the fact that elections officials around the country uniformly have responded to the misinformation that the President has shared with the right information.

I think what is important, and as we speak about elections going forward, is not to be thinking about defensive procedures, but offensive. We need to engage our communities in the civic education and inoculation that would protect them from being affected by this misinformation.

Ms. JACKSON LEE. Thank you very much.

In 2016, Russia was blamed for breaching 21 local and State election systems. In fact, Robert Mueller released indictments of 13 Russians regarding interference in our 2016 elections.

Mr. Levine, what should we be focusing on? What, if any, has the Marshall Fund seen that should be done regarding the outside international interference in our elections which is predicted to be extensive in 2020? Mr. Levine.

Mr. LEVINE. Sure, Congresswoman, thank you for that important question. I will make a couple of points to your question that I think are worth noting.

No. 1, I think that election officials need to have Plan A and Plan B. For almost every cyber component of our election infrastructure there can be an analog piece that can be available to use so that in the event of any kind of cyber event we have something to fall back on.

We have seen this happen a number of ways. We know that for those States and communities that use electronic poll books or electronic lists of voters to check in, if there is either a technical glitch or, in fact, a nefarious act, we know that if people have paper poll books they can continue that voting process.

We know that with regards to election night reporting websites, we know if that a website is to go down, for example, because of a denial-of-service attack, that if folks can have redundant websites where they can have other means to be able to share that information, that could help ensure that there is voter confidence.

So making sure that folks have things like additional ballots, paper poll books, redundant websites. As we look now, we probably are seeing an increase in folks that, for example, are requesting absentee ballots on-line. Making sure that, in fact, if you can't make such a request, that maybe you have a fillable PDF form so that you are still able to have that request through. I think that is really, really important.

I think the second piece that I think is worth noting really quickly is that it is really important that the information from the intelligence and law enforcement community about the threats as much as possible is being shared with State election officials and subsequently with the American public so that as much as possible the American public has the opportunity to prepare accordingly, whether it is the misinformation and any other threats.

Ms. JACKSON LEE. Thank you so very much.

Mr. Gilligan, if you would just give quickly one significant action that Congress can take regarding internet security in the voting process. Mr. Gilligan?

Mr. GILLIGAN. Thank you, Congresswoman.

Let's see. If I were to think of one thing that Congress could do, I think what I would suggest is the following, and we have seen indications of it in some of the comments from the Members. That is, when we address the security of local elections offices, we have to realize that they are underresourced and don't have the talent that the State level and the larger elections jurisdictions do.

So what I think is going to be important going forward is we cannot assume that local elections offices are ever going to be able to protect themselves. We actually have to do it for them.

This is a discussion that we are having with the State-level organizations. I mentioned in my testimony some capabilities that we are working to deploy with CISA and the elections community.

That, in fact, is sort-of we can do it and we can deploy it without a whole lot of support from the local elections offices and actually protect them. One of them is this endpoint detection and response. The other is this malicious domain blocking and reporting.

So I think what then the recommendation that I would make to Congress is, if Congress could help in the funding of these initiatives to get them off the ground, to get enough of it deployed, ultimately what we have seen in other situations, the States will start

to kick in funding over time. But to get the ball rolling, Federal funding is very helpful.

So thank you.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman. Thank you. I yield back.

Mr. RICHMOND. The gentlelady from Texas has yielded back.

I now recognize the gentlelady from New York, Miss Rice, for 5 minutes.

Miss RICE. Thank you, Mr. Chairman.

I would ask, put this question out to all of the witnesses. I believe, Ms. McReynolds, you were talking about how things are done in your State of Colorado. What State or locality does mail-in-ballot voting really well? Like what system can we emulate?

We in New York have done this for a long time, but we had a historically very difficult time in our June primary. It actually took 5 weeks to certify one of—a Congressional primary. We think of ourselves in New York as pretty progressive when it comes to these issues.

So who can we look to? We still have 3½ months before people go to the—September, October—no, 3, 3 months before people go to the polls. So maybe if you could just expound on who you think does it really well.

Ms. MCREYNOLDS. Sure. Thank you for the question, Congresswoman.

Yes, I mean, we saw issues in New York. I think that New York actually has lagged behind many States in terms of updating policies around voting access. There hasn't been early voting. There wasn't no-excuse absentee up to this point. There have really been a lot of issues in New York. Exorbitantly long lines actually back in 2018 and even prior to that. So there have been issues there, and I think there is some updating of policies that definitely needs to happen.

In terms of my expert opinion on sort-of the work I did in Colorado and then the work I have now done with various States, I think no State—it is not necessarily a cookie-cutter approach. However, what we have in front of us is a good example of a slew of States that have implemented various policies in the last few years that have improved their processes, improved the system for voters, and also enhanced security.

Colorado is one of them. California adopted a model that looks very much like Colorado. Utah has expanded their voting-at-home program to be now for the entire State, and they have emulated some of those good practices from Colorado, as well as Oregon and Washington.

Miss RICE. So what are those practices, if you can just tell us? What are those, just if you can give us——

Ms. MCREYNOLDS. Sure. So a couple of things that we did in Colorado that I think are good to emulate.

One is modernizing registration. So we have automatic registration. We automatically update addresses based on moves that we get from the motor vehicle locations or from the United States post office. We literally consume that data monthly, update addresses. So Colorado, for instance, and many of the States in the West, have the cleanest voter files in the country.

We also have created systems like ballot tracking. So ballot tracking started in Denver, Colorado, way back in 2009. That is a notification system just like tracking a package where you get a text or email about when your ballot goes out, when it is on its way to you, and then confirmation when the election official receives it.

That is one of the top-level recommendations that States can do right now. There is technology available. It doesn't require a lot of change in any State. You can literally adopt it as a service to voters and it enhances security, and it is one of our top-level recommendations.

The final recommendation I would say is expanding drop-off options for voters. So at secure 24-hour drop boxes, at drive-up drop-off, there are examples of drive-up drop-off just like a drive-thru line at a restaurant. You can drop off your ballot through the window of your car and not have to get out, not have to interact with anybody.

Then, finally, expanding drop-off options to accept mail ballots at all voting locations. Not every State allows you to drop your ballot off at a polling place.

Those are examples. Those drop-off options and ballot tracking can be done now, can be adopted now across the country, and there is time to do that.

Miss RICE. Can I also ask you, because there are going to be some people who actually want to go to the polls.

Ms. MCREYNOLDS. Yes.

Miss RICE. I know New York is not unique. Most of our poll watchers are people who are in that vulnerable age bracket who may not want to be sitting at a poll for 12 hours in November, God forbid that we are where we are still with this virus.

So what would you suggest to improve. I mean, obviously, it doesn't help that people are closing down polling locations. Other than keeping as many open as possible, what would you suggest to secure people who prefer to vote in person?

Ms. MCREYNOLDS. Yes. I mean, in-person voting has to exist, but we have to think about it in a different way than we have ever thought about it before. What I mean by that is we need, for instance, the business community to step up and offer locations.

One of the things that is happening now, which I am sure many of you have seen, is there is this concept of arenas, large sports facilities being used as polling places. Kentucky used their State fairgrounds and were able to serve tens of polling places all in one place with social distancing.

So these sort-of large locations are really important. I have suggested car dealerships. I think car dealerships in the showrooms and the accessibility of them, given where they are usually located, would be excellent locations in many of the big cities.

So we have to be creative. I think the business community can really help solve a lot of these challenges, whether they offer a polling place, offer their workers to help on election day, or offer their location to be even a drive-up drop-off. Even a drive-up drop-off would be tremendously helpful in States.

So this is kind-of an all-of-community type of response that we really need to see happen to make sure that our vote is protected.

Miss RICE. Thank you very much.

Mr. Chairman, I yield back.

Mr. RICHMOND. The gentlelady from New York has yielded back.

I now recognize the gentlelady from Illinois, Ms. Underwood, for 5 minutes.

Ms. UNDERWOOD. Thank you, Mr. Chairman.

The integrity of our elections is essential to the preservation of our Republic. Securing our elections is a major concern for my constituents in Illinois, where the personal information of 76,000 voters was accessed by Russian operatives in 2016.

We must immediately invest in our election infrastructure to protect our democracy against on-going attempts to interfere.

On top of those preexisting threats, the COVID–19 pandemic has heightened the need for greater flexibility in how, when, and where people vote. Nobody should be forced to choose between protecting their health and exercising their Constitutional rights.

Elections security is National security, and I am grateful to our witnesses for advising this committee on how to protect it, whether that means preventing foreign interference or conducting safe and accessible elections during a pandemic.

Ms. Albert, one result of the pandemic—or rather a result of this administration's failure to adequately respond to the pandemic and support families during this crisis—is a surge in housing instability. Many Americans are out of work and at risk of losing their homes, whether they rent or own. Suddenly a lot of people's addresses may soon be out of date.

How can we protect the voting rights of people experiencing housing instability during this crisis and make sure that they are not subject to unnecessary voter registration purges?

Ms. ALBERT. Thank you for the question, Congresswoman.

As we have talked about before, H.R. 1 contains many different provisions that would be beneficial in moments like this. I think the thing that we have seen in this pandemic is that our system is not as flexible and comprehensive as it could be in order to meet the needs of different communities.

So, for example, communities who are experiencing housing displacement right now, homeless communities, they are strongly benefited by same-day registration or, in addition, provisions that allow for updating registration at the polling location.

To be clear, I mean real same-day registration, which means you can go to your voting polling location and update your address and it is not you have to go downtown to the main office that is only open between 9 and 3 on election day in order to update your address.

Ms. UNDERWOOD. Right.

Ms. ALBERT. Really what we are seeing is that those vulnerable communities are just more vulnerable in this situation and are really dealing with much more than they ever have before.

So not only do we need to be looking at this now, but we really should be modernizing our system for the next disaster, for the next pandemic, for the next hurricane to really meet the needs of our constituents.

Ms. UNDERWOOD. Mr. Levine and Ms. McReynolds, do you believe voting from home could help these displaced voters? If so, what does the Federal Government need to do right now to make

sure that Americans are able to vote from home, even if their address changes within the next few months?

Ms. MCREYNOLDS. Sure. I can answer that.

One thing I would say about what we did in Colorado is we created this system of same-day registration, combined with automatic registration, combined with mailing a ballot to all electors. So we have a process and tried to create and fill all those gaps.

But then we also created the concept of vote centers, and that started in Colorado, as well as an innovation that allows a voter to go to any of the locations and update their address or what have you.

That really reduced provisional ballots by 98 percent and converted those to normal ballots, because most of the people that would show up at the wrong polling place was because of an address change.

So we created a new way to deal with in-person voting that has significantly improved the voting experience.

So vote centers is also a really great concept. The one thing I would say about vote centers is it does require technology. It is going to be a much bigger lift to set up ahead of November because there is a short period of time. But there still is a way to handle provisionals and all of those sorts of things should somebody not receive their mail ballot.

The other aspect I would say is that it is critically important before every election that voters check their registration, make sure they are active, make sure their address is up-to-date. Then if something does go awry with their mail ballot not arriving, that they utilize the processes that are in place in various States—and I am from Illinois, so I am also familiar with the Illinois provisions—and make sure that voters are familiar with what they can do to take action should they not receive their ballot.

In every single State you can still vote in person, you still have that provisional ballot as a safeguard should something happen that makes it difficult for you to receive your ballot.

Ms. UNDERWOOD. Well, Mr. Levine, I am out of time.

But thank you so much to all of our witnesses for being here. We appreciate this information and your testimony before our committee.

Mr. Chairman, I yield back.

Mr. RICHMOND. The gentlelady from Illinois has yielded back.

I want to thank the witnesses for their valuable testimony and the Members for their questions.

The Members of the subcommittee may have additional questions for the witnesses, and we ask that you respond expeditiously in writing to those questions. Without objection, the committee record shall be kept open for 10 days.

Hearing no further business, the subcommittee stands adjourned.

Thank you all.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman.

[Whereupon, at 11:40 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM HONORABLE JAMES R. LANGEVIN FOR SYLVIA ALBERT

Question 1a. In your testimony, you raised the issue of accessibility for voters with disabilities and expressed that voters with disabilities in Pennsylvania had difficulty casting their votes in the 2020 primary.

What barriers to voting exist for people with disabilities, and how have barriers increased since the public health crisis began?

Answer. Response was not received at the time of publication.

Question 1b. What solutions should we be considering now to avoid denying people with disabilities the right to vote in November?

Answer. Response was not received at the time of publication.

QUESTIONS FROM HONORABLE JAMES R. LANGEVIN FOR JOHN GILLIGAN

Question 1. I have been convinced for some time that cybersecurity concerns associated with on-line voting are simply too great and the stakes too high to be comfortable with that idea. Yet a handful of States are considering this in light of the challenges that come with voting in person during a global pandemic.

What is your position on on-line voting?

Answer. On-line voting, which we define as the electronic return of a voted ballot from a voter's device, poses unique and complex technical challenges. At present, the technologies needed to ensure on-line voting is not susceptible to malicious or inadvertent compromise do not exist. As such, presently or in the near future, CIS does not recommend the use of on-line voting for U.S. elections. The exception to this recommendation would be in very limited circumstances where the risks of on-line voting are outweighed by other risk factors such as the potential disenfranchisement of eligible voters who have no other means to cast their vote, e.g., the voting of overseas military personnel. Even in these limited circumstances, extraordinary care must be applied to ensure confidentiality and integrity of the electronic ballot as well as proper identification and authentication of the voter.

In the longer term, the potential of secure on-line voting to increase voter participation is appealing, if done securely. However, the unique requirements for secure on-line voting exceed those required for on-line banking or other on-line transactions whose threats and mitigations have been tested over time. This is driven by several factors; the most difficult is ensuring that the contents of a cast ballot are a secret to everyone except the voter while verifying that it is received and tabulated correctly. Identifying and correcting an error is particularly difficult as the election office can only know that the voter cast a ballot and not its contents. This is substantially more complicated than a financial transaction and unlike any other transaction commonly conducted on-line. As such, on-line voting must be addressed with new and different approaches.

Fortunately, there is a group of researchers from academia and industry who are working on technical solutions to make on-line voting secure. While there remain issues, the currently preferred technical approach promoted by these researchers is known as End-to-End Verifiable (E2E–V) solutions. With this approach, voters and the public are provided assurances that the votes were cast, recorded, and counted properly regardless of the medium used. Otherwise, the voter or an auditor is alerted. As such, E2E–V provides hope that on-line voting can be done securely at some point in the future.

Question 2. What would need to happen in order for this on-line voting to be a viable solution? Can these steps be implemented before the 2020 elections?

Answer. As noted above, further research, development, and testing using end-to-end verifiable on-line voting approaches, or alternative technical approaches, will be necessary before on-line voting can be considered viable. In particular, researchers need to solve conflicts between the verifiability of the voting process and other re-

quirements such as usability and accessibility. This will take time and significant investment. Moreover, given the critical nature of voting, extensive piloting and transparent examination by experts must be accomplished before on-line voting solutions can be deemed safe and secure. It is not possible to accomplish these efforts prior to the November 2020 election.