SECURING DEMOCRACY: PROTECTING AGAINST THREATS TO ELECTION INFRASTRUCTURE AND VOTER CONFIDENCE

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

JANUARY 20, 2022

Serial No. 117–41

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

47–316 PDF WASHINGTON : 2022

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
DONALD M. PAYNE, JR., New Jersey
J. LUIS CORREA, California
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
ERIC SWALWELL, California
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California
JOSH GOTTHEIMER, New Jersey
ELAINE G. LURIA, Virginia
TOM MALINOWSKI, New Jersey
RITCHIE TORRES, New York
JOHN KATKO, New York
MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
JEFFERSON VAN DREW, New Jersey
RALPH NORMAN, South Carolina
MARIANNETTE MILLER-MEEKS, Iowa
DIANA HARSHBARGER, Tennessee
ANDREW S. CLYDE, Georgia
CARLOS A. GIMENEZ, Florida
JAKE LATURNER, Kansas
PETER MEIJER, Michigan
KAT CAMMACK, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York

HOPE GOINS, *Staff Director*
DANIEL KROESE, *Minority Staff Director*
NATALIE NIXON, *Clerk*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

YVETTE D. CLARKE, New York, *Chairwoman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
ELISSA SLOTKIN, Michigan
KATHLEEN M. RICE, New York
RITCHIE TORRES, New York
BENNIE G. THOMPSON, Mississippi *(ex officio)*
ANDREW R. GARBARINO, New York, *Ranking Member*
RALPH NORMAN, South Carolina
DIANA HARSHBARGER, Tennessee
ANDREW CLYDE, Georgia
JAKE LATURNER, Kansas
JOHN KATKO, New York *(ex officio)*

MOIRA BERGIN, *Subcommittee Staff Director*
AUSTIN AGRELLA, *Minority Subcommittee Staff Director*
MARIAH HARDING, *Subcommittee Clerk*

CONTENTS

SECURING DEMOCRACY: PROTECTING AGAINST THREATS TO ELECTION INFRASTRUCTURE AND VOTER CONFIDENCE

Thursday, January 20, 2022

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 2:02 p.m., via Webex, Hon. Yvette D. Clarke [Chairwoman of the subcommittee] presiding.

Present: Representatives Clarke, Jackson Lee, Langevin, Slotkin, Garbarino, Harshbarger, Clyde, and LaTurner.

Chairwoman CLARKE. The Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation will come to order. The subcommittee is meeting today to receive testimony on "Securing Democracy: Protecting Against Threats to Election Infrastructure and Voter Confidence." Without objection, the Chair is authorized to declare the committee in recess at any point.

Good afternoon, everyone. I would like to thank our panel of witnesses for participating in today's hearing on how we can secure our democracy against threats to election systems, as well as efforts to undermine voter confidence and faith in democratic institutions.

So much has changed since this committee held its first dedicated election security hearing in 2019, which was already about 2 years too late. That is because in 2017, as the rest of us were waking up to grave security threats posed to our Nation's underfunded, outdated voting systems, Republicans controlled the House. Despite multiple requests by the committee Democrats to hold hearings on election security, the Republican Chairman largely declined to do so, except for a single hearing on threats to elections and other critical infrastructure.

Still, Democrats got to work. The Democratic Task Force on Election Security worked to find solutions and make investments to help State and local officials upgrade and improve systems. When Democrats regained control of the House in 2019, this work did not cease, it accelerated.

We secured funding for election upgrades at the State level and built up capacity at the Federal level, empowering CISA to work with election officials, vendors, and other stakeholders to harden

voting systems around the country. At the end of the day, we made enormous progress. Roughly 96 percent of voters used voter-verifiable paper ballots and the results were validated by legitimate, credible post-election audits in every swing State.

Election security experts called the 2020 election the most secure in American history in a year with historically high turnout during a global pandemic. It is hard to square that with what happened next. The out-going President ratcheted up the disinformation campaign he had been carrying out in the open for weeks. Rather than accept his loss gracefully, the former President asked his loyalists to subscribe to baseless claims of voter fraud at a scale never seen in history to explain his defeat.

Despite the obvious absurdity and total lack of evidence, former President Trump was somehow able to parlay this message into a campaign so effective that he convinced 145 Republican Members of this very chamber to vote against certification of the election results. That same day, thousands of Trump supporters mobbed the U.S. Capitol with nooses, bear spray, and zip ties, inflicting serious or even fatal injuries on Capitol Police officers sent here to protect and serve.

We as a Nation will be dealing with the fallout from the 2020 election for a long time to come. Today, election denialists are running for office across the country and State legislatures are pursuing fake, partisan audits and restrictive voting laws that will do nothing more than create another barrier for voters of color to cross to cast their vote. Recent polls suggest that 1 in 3 voters question the legitimacy of the 2020 election and 1 in 3 election officials feels unsafe in their job.

I began this statement by talking about the efforts of Democrats to secure elections, not as a pat on the back or to inflame partisan divisions, but rather because I believe we are at an inflection point in our Nation's history where terms like "election security" and "election integrity" are being weaponized in ways that I have never seen before.

As long as we are opening up the proper scope of those terms, let me tell you how I define election security. No. 1, making sure that every eligible voter who wants to cast a vote is able to cast it; and, No. 2, making sure that vote is counted as it was cast. Anything that undermines either of these tenets, whether that is restrictive voting laws, disinformation that threatens the health of our republic, or outdated voting machines that can be exploited by hackers, is a threat to election security. That is why this hearing will cover the waterfront of issues that threaten secure elections today, even those outside the realm of cybersecurity.

I am also profoundly concerned about the fractured state of our information ecosystem and the ability for media consumers to simply choose their own reality based on the Facebook groups they join and the cable news outlets they choose to watch. This is a major existential threat to our democracy, and I look forward to hearing from this panel to see how we might start to rebuild faith in democratic institutions.

Finally, I believe the Federal Government, and CISA in particular, has a role to play in confronting the mis- and disinformation narratives that jeopardize our faith in free and fair

elections and other issues that threaten our National security, public health, and safety. That is why I am introducing legislation to authorize CISA to identify, track, and address mis- and disinformation through efforts like the Rumor Control website.

The best way to attack a lie is with the truth. I hope my colleagues on both sides of the aisle will join me in supporting CISA's efforts to prebunk and debunk the kind of disinformation that erodes our democracy.

I thank our panel of witnesses for participating today and I look forward to a robust discussion.

[The statement of Chairwoman Clarke follows:]

STATEMENT OF CHAIRWOMAN YVETTE D. CLARKE

JANUARY 20, 2022

Good afternoon. I would like to thank the witnesses for participating in today's hearing on how we can secure our democracy against threats to election systems, as well as efforts to undermine voter confidence and faith in democratic institutions.

So much has changed since this committee held its first, dedicated election security hearing in 2019—which was already about 2 years too late.

That's because in 2017—as the rest of us were waking up to grave security threats posed to our Nation's under-funded, outdated voting systems—Republicans controlled the House.

And, despite multiple requests by committee Democrats to hold hearings on election security, the Republican Chairman largely declined to do so—except for a single hearing on threats to elections and other critical infrastructure.

Still, Democrats got to work. The Democratic Task Force on Election Security worked to find solutions and make investments to help State and local officials upgrade and improve systems.

And when Democrats regained control of the House in 2019, this work did not cease—it accelerated.

We secured funding for election upgrades at the State level, and built up capacity at the Federal level—empowering CISA to work with election officials, vendors, and other stakeholders to harden voting systems around the country.

At the end of the day, we made enormous progress.

Roughly 96 percent of voters used voter-verifiable paper ballots—and the results were validated by legitimate, credible post-election audits in every swing State.

Election security experts called the 2020 election the "most secure in American history"—in a year with historically high turnout, during a global pandemic.

It's hard to square that with what happened next.

The out-going President ratcheted up the disinformation campaign he'd been carrying out, in the open, for weeks.

Rather than accept his loss gracefully, the former President asked his loyalists to subscribe to baseless claims of voter fraud, at a scale never seen in history, to explain his defeat.

Despite the obvious absurdity and total lack of evidence—former President Trump was somehow able to parlay this message into a campaign so effective that he convinced 145 Republican Members of this very Chamber to vote against certification of the election results.

That same day, thousands of Trump supporters mobbed the U.S. Capitol with nooses, bear spray, and zip ties—inflicting serious or even fatal injuries on Capitol Police officers sent here to protect and serve.

We, as a Nation, will be dealing with the fallout from the 2020 election for a long time to come.

Today, "election denialists" are running for office across the country, and State legislatures are pursuing fake, partisan audits and restrictive voting laws that will do nothing more than create another barrier for voters of color to cross to cast their vote.

Recent polls suggest that 1 in 3 voters question the legitimacy of the 2020 election. And, 1 in 3 election officials feels unsafe in their job.

I began this statement by talking about the efforts of Democrats to secure elections—not as a pat on the back or to inflame partisan divisions.

But rather, because I believe we are at an inflection point in our Nation's history—where terms like "election security" and "election integrity" are being weaponized in ways that I have never seen before.

As long as we're opening up the proper scope of those terms, let me tell you how I define election security: (1) Making sure that every eligible voter who wants to cast a vote is able to cast it, and (2) making sure that vote is counted as it was cast.

Anything that undermines either of those tenets—whether that's restrictive voting laws, disinformation that threatens the health of our republic, or outdated voting machines that can be exploited by hackers—is a threat to election security.

That is why this hearing will cover the waterfront of issues that threaten secure elections today—even those outside the realm of cybersecurity.

I am also profoundly concerned about the fractured state of our information ecosystem—and the ability of media consumers to simply choose their own reality based on the Facebook groups they join and the cable news outlets they choose to watch.

This is a major, existential threat to our democracy—and I look forward to hearing from this panel to see how we might start to rebuild faith in democratic institutions.

Finally, I believe the Federal Government—and CISA in particular—has a role to play in confronting the mis- and disinformation narratives that jeopardize our faith in free and fair elections, and other issues that threaten our National security, public health, and safety.

That is why I am introducing legislation to authorize CISA to identify, track, and address mis- and disinformation through efforts like the Rumor Control website.

The best way to attack a lie is with the truth, and I hope my colleagues on both sides of the aisle will join me in supporting CISA's efforts to "prebunk" and debunk the kind of disinformation that erodes our democracy.

I thank the witnesses for participating today, and look forward to a robust discussion.

Chairwoman CLARKE. The Chair now recognizes the Ranking Member of the subcommittee, the gentleman from New York, Mr. Garbarino, for an opening statement.

Mr. GARBARINO. Thank you, Chairwoman Clarke. Thank you very much for holding this hearing today. I appreciate our witnesses being here to discuss how we can support our State and local officials, secure election infrastructure from cyber threats, and examine ways to improve the tools and services provided by the Cybersecurity and Infrastructure Security Agency.

In 2021, our Nation experienced an unprecedented number of cyber attacks against our critical infrastructure. We began 2021 by analyzing the impacts of the SolarWinds cyber espionage campaign and we ended the year by responding to Log4j, the most pervasive vulnerability the cybersecurity community has ever seen. This is not to mention the dozens of significant ransomware attacks throughout the year.

On top of spikes in cyber crime, we are seeing a lack of faith among voters in our election security. As we enter 2022, we must keep a keen eye on the mid-term elections and ensure that voters can be confident that their vote will count. Given the volume and sophistication of cyber threats we face, we must empower CISA with the tools and resources it needs to support our State and local election officials so that they can carry out their mission to administer free and fair elections.

CISA's election security mission has greatly evolved since election infrastructure was designated as a subsector of our Nation's critical infrastructure in 2017. CISA has gone to great lengths to build trusted relations with the State and local election officials across the country and is providing free and voluntary cybersecurity services, tools, and other guidance in all 50 States.

A key part of securing election infrastructure that is owned and operated by State and locals is ensuring that CISA has the ability to provide situational awareness about vulnerabilities across digital footprints. Initiatives like CISA's Crossfeed program are a commendable effort in this respect. Crossfeed leverages the best available technology to attribute public-facing assets to the organizations that own them, and provides CISA the ability to quickly detect new vulnerabilities. You can't secure what you can't see, and this real-time common operating picture, as well as several other CISA programs, continue to provide great value to State and local officials across the country.

I am pleased that we are joined today by Matt Masterson, who led CISA's election security work in the prior administration and built the backbone of the trusted relationships that CISA leverages today. Matt is experienced in elections at every level, from administering them at the State level in Ohio to serving as commissioner of the Election Assistance Commission and as senior cybersecurity advisor for elections at CISA. I look forward to hearing from Matt about the practical, meaningful steps we can take to improve CISA's ability to support our State and local officials. I am determined to work with the State and local officials and other stakeholders in New York's Second Congressional District and across the country to improve their cybersecurity posture in the wake of increasing threats.

This past August, I was pleased to host a roundtable discussion in my district with local government, critical infrastructure stakeholders, and CISA's Region 2 team where CISA presented numerous tools and resources that they can provide to bolster critical infrastructure security free of charge. I am also proud to have been an original cosponsor of the Chairwoman's State and Local Cybersecurity Improvement Act, which was signed into law last year.

I hope we can all agree more resources for our State and local governments are necessary. We must also ensure these funds are spent responsibly and have a meaningful impact on risk reduction. CISA plays a vital role. This important bill is a tremendous step forward in our fight to enhancing election infrastructure security at a local level.

I look forward to hearing from our witnesses today about how Congress can bolster CISA's role in election security and how CISA can turn support—in turn support our State and local election officials.

Thank you, Madam Chair, and I yield back.

[The statement of Ranking Member Garbarino follows:]

STATEMENT OF RANKING MEMBER ANDREW GARBARINO

Thank you, Chairwoman Clarke, for holding this hearing today. I appreciate our witnesses being here to discuss how we can support our State and local election officials, secure election infrastructure from cyber threats, and examine ways to improve the tools and services provided by the Cybersecurity and Infrastructure Security Agency (CISA).

In 2021, our Nation experienced an unprecedented number of cyber attacks against our critical infrastructure. We began 2021 by analyzing the impacts of the SolarWinds cyber espionage campaign, and we ended the year by responding to Log4j—the most pervasive vulnerability the cybersecurity community has ever seen. This is not to mention the dozens of significant ransomware attacks throughout the year.

On top of spikes in cyber crime, we are seeing a lack of faith among voters in our election security. As we enter 2022, we must keep a keen eye on the mid-term elections and ensure that voters can be confident that their vote will count. Given the volume and sophistication of the cyber threats we face, we must empower CISA with the tools and resources it needs to support our State and local election officials so that they can carry out their mission to administer free and fair elections.

CISA's election security mission has greatly evolved since election infrastructure was designated as a subsector of our Nation's critical infrastructure in 2017. CISA has gone to great lengths to build trusted relationships with State and local election officials across the country, and has provided free and voluntary cybersecurity services, tools, and other guidance in all 50 States.

A key part of securing election infrastructure that is owned and operated by State and locals is ensuring that CISA has the ability to provide situational awareness about vulnerabilities across digital footprints. Initiatives like CISA's Crossfeed Program are a commendable effort in this respect. Crossfeed leverages the best available technology to attribute public-facing assets to the organizations that own them, and provides CISA the ability to quickly detect new vulnerabilities. You can't secure what you can't see, and this real-time common operating picture, as well as several other CISA programs, continue to provide great value to State and local officials across the country.

I am pleased that we are joined today by Matt Masterson, who led CISA's election security work in the prior administration and built the backbone of the trusted relationships that CISA leverages today. Matt has experience in elections at every level, from administering them at a State level in Ohio, to serving as commissioner of the Elections Assistance Commission, and as senior cybersecurity advisor for elections at CISA. I look forward to hearing from Matt about the practical, meaningful steps we can take to improve CISA's ability to support our State and local officials.

I am determined to work with State and local officials, and other stakeholders in New York's 2nd district and across the country to improve their cybersecurity posture in the wake of increasing threats. This past August, I was pleased to host a roundtable discussion in my district with local government, critical infrastructure stakeholders, and CISA's Region 2 team, where CISA presented numerous tools and resources they can provide to bolster critical infrastructure security, free of charge.

I am also proud to have been an original cosponsor of the Chairwoman's State and Local Cybersecurity Improvement Act, which was signed into law last year. While we can all agree more resources for our State and local governments are necessary, we must also ensure these funds are spent responsibly and have a meaningful impact on risk reduction. CISA plays a vital role here. This important bill is a tremendous step forward in our fight to enhance election infrastructure security at the local level.

I look forward to hearing from our witnesses today about how Congress can bolster CISA's role in election security and how CISA can in turn support our State and local election officials. Thank you, Madam Chair.

Chairwoman CLARKE. I thank our Ranking Member for his opening statement. Just to remind Members that the subcommittee will operate according to the guidelines laid out by the Chairman and Ranking Member in their February 3 colloquy regarding remote procedures. Member statements may be included for the record.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

JANUARY 20, 2022

Good afternoon. I want to thank Chairwoman Clarke and Ranking Member Garbarino for holding this important hearing on election security as we enter a mid-term election year.

Ensuring the security of our elections has been a priority for me, particularly since 2016, where we witnessed unprecedented foreign interference in our electoral process.

In the 115th Congress, then-House Administration Committee Ranking Member Robert Brady and I formed the Congressional Task Force on Election Security.

The Task Force produced a report with 10 recommendations for enhancing our Nation's election security and led to the introduction of the Election Security Act to implement these important proposals.

Unfortunately, while the House has passed these critical election security provisions as part of broader election reform legislation, unified Republican opposition has blocked passage in the Senate.

Although we have been unable to pass these critical provisions, Democrats have been able to secure over $1 BILLION in support to the States, including through the CARES Act, to enhance the security of voting systems.

Combined with the work of the Cybersecurity and Infrastructure Security Agency and other Federal partners, we were able to have the most secure election in American history in 2020, even amidst a global pandemic.

That achievement speaks volumes about the hard work of election officials throughout the country and the potential to protect our elections when we collaborate to prioritize security.

We must build on this progress by investing additional resources in election security, replacing paperless voting machines with paper ballots, conducting evidence-based post-election audits, and ensuring the highest security standards for voter registration databases, electronic poll books, and other election technology.

Unfortunately, the aftermath of the 2020 election demonstrated that even when an election is highly secure, misinformation can produce devastating consequences for our democratic system of government.

If people are convinced that an election result is illegitimate—no matter how baseless that claim may be—we have seen first-hand the violence it can produce.

With social media enabling misinformation to spread at unprecedented speeds, developing strategies to respond and contain such falsehoods will require innovative solutions to address this very complex problem.

I applaud Chairwoman Clarke for her efforts to authorize CISA's disinformation efforts, particularly its Rumor Control website to debunk misinformation promptly.

An essential aspect of addressing misinformation is to promote accurate information from trusted sources, and I am confident that this legislation can help achieve that goal.

I look forward to working with her to move this important bill forward.

The past few years has been a troubling time for our democracy.

We have seen people spread lies about the integrity of our elections and use them to justify new restrictive voter laws that do nothing to enhance voter confidence.

Instead, they only make it harder for Americans, and particularly people of color, to exercise their fundamental right to vote.

That only further erodes trust in our institutions and makes our democracy more vulnerable.

Fortunately, there is another way, as reflected in the Freedom to Vote: John R. Lewis Act that the House passed last week.

This approach ensures voting is accessible to all who are eligible and invests in meaningful election security, helping to build confidence in the integrity of our elections.

We have not been able to enact this important legislation, but we will continue to fight, as the consequences of failure on this issue are simply too high.

The panel of witnesses we have today are all individuals who have been working tirelessly in recent years to address these challenges.

I look forward to hearing their ideas about how we can expand on our successes so far, continue to strengthen the security of our election infrastructure, and build back public confidence in our democratic institutions.

I yield back.

Chairwoman CLARKE. Right now I am going to move us to our panel. When and if our Ranking Member or Chairman arrive, we will hear from them.

I now welcome our panel of witnesses.

First, I would like to welcome Ms. Gowri Ramachandran, excuse me. Ms. Ramachandran serves as senior counsel in the Brennan Center's democracy program, where her work focuses on election security, election administration, and combatting election disinformation. Prior to her role at the Brennan Center, Ms. Ramachandran, excuse me, was professor of law at Southwestern Law School in Los Angeles, California.

Second, we will hear from Mr. Alex Stamos, the director of the Stanford Internet Observatory. At Stanford he oversaw the Election Integrity Partnership, a coalition of researchers, civil society

groups, and other stakeholders working to track and respond to election disinformation in real time. Mr. Stamos also serves as a commissioner on the Aspen Institute's Commission on Information Disorder and is the former chief security officer for Facebook.

Next we have Mr. Ezra Rosenberg, who has served as the co-director of the Voting Rights Project at the Lawyers' Committee for Civil Rights Under Law since July 2015. Mr. Rosenberg joined the Lawyers' Committee in November 2014 as special senior counsel in the Legal Mobilization Project, continuing a 40-year career in the public and private sectors.

Finally, I would like to welcome Mr. Matt Masterson, who serves as a nonresident policy fellow with the Stanford Internet Observatory. Prior to his current role, Mr. Masterson was a senior cybersecurity advisor at the Department of Homeland Security, where he focused on election security issues. He has also served as the commissioner at the Election Assistance Commission and on the staff of the Ohio Secretary of State's Office.

Without objection, the witnesses' full statements will be inserted in the record. I now ask each witness to summarize his or her statement for 5 minutes, beginning with Ms. Ramachandran. Thank you for joining us.

STATEMENT OF GOWRI RAMACHANDRAN, SENIOR COUNSEL, BRENNAN CENTER FOR JUSTICE

Ms. RAMACHANDRAN. Chairwoman Clarke, Ranking Member Garbarino, and Members of the committee, thank you for the opportunity to discuss election security.

The November 2020 election is widely considered the most secure in American history. But an anti-democracy movement, fueled by the Big Lie, poses serious threats to elections. Taking these threats seriously requires expanding upon recent improvements to election security.

In my testimony I will cover 3 topics. First, I will describe what went right in 2020. State and local election security, CISA, the EAC, and voters themselves all played a role with support from Congress helping to make it possible.

Second, I will describe the threats that the election sabotage movement is posing to election infrastructure. Lies about the 2020 election not only undermine voter confidence, they also lead to tangible security risks to election systems and increase the risk of insider attacks.

Third, I will address how election infrastructure can be bolstered against this threat with financial resources and incentivizing true election integrity measures, like risk-limiting audits and rigorous election vendor security standards.

In 2016, 1 in 5 voters cast their vote using a paperless voting system. But in 2020, an estimated 96 percent of voters used paper ballots. In fact, no swing State used paperless voting machines and routine statutory tabulation audits were performed in every swing State. None found discrepancies that would have been sufficient to alter the outcome of the Presidential election.

In addition to this crucial move away from paperless systems, CISA expanded its collaboration with State and local election officials. It provided vulnerability testing and trainings, shared infor-

mation, and emphasized public education. For instance, in the fall of 2020, some Florida voters received threatening emails in the guise of a domestic far-right group that has promoted violence. The intelligence community detected the true source of the attack, alerted election officials, and held a joint press conference to let the public know the truth: The emails were actually coming from malicious actors associated with Iran.

Election officials adopted resiliency measures, such as stocking emergency paper ballots in case of machine failure, to ensure that voters could exercise their rights even when there was sporadic polling place problems. In some States, the many options for voting served as their own resiliency measure against the pandemic. These options allowed voters to spread themselves out among different voting methods and days. It also meant that money from Congress was crucial.

After this success, what lies ahead? The continued lie that the 2020 election was stolen is not only undermining the public's confidence, but is also threatening election infrastructure directly through sham partisan reviews and insider threat risks.

Sham partisan reviews have provided unmonitored election equipment access to biased, uncertified partisans. In fact, decertification or decommission of equipment has been necessary after multiple sham reviews across the country. Ballot security breaches have also been damaging.

Anti-democratic forces are also undermining a once broadly-shared commitment to competent and nonpartisan election administration. Many election officials committed to fair elections are resigning or being pushed out in the fact of myriad attacks and pressures.

Moreover, given that almost one-third of Americans still believe the Big Lie, it is unsurprising that some minority of election officials, and likely even some employees and vendors who support their work, themselves buy into election conspiracy theories. Unprecedented amounts of money are being spent in campaigns for election administration jobs with election denialism, for and against, being treated as a key issue.

What happens if officials and election personnel fall victim to these falsehoods? We are witnessing the first glimpses now. In Colorado, a county clerk with connections to election conspiracy theorists gave unauthorized access to the county's voting systems. Photos of passwords for the voting machine software ended up online.

These security risks are alarming, but they can be mitigated. It should go without saying that all levels of law enforcement should enforce existing laws against threats, especially when election personnel are intimidated. Congress can work to combat doxing and provide for physical security and training. When it comes to insider threats, well-accepted best practices already exist. They include restricting and logging access to critical systems, monitoring through video surveillance, background checks, and choosing vendors that also employ good practices.

This all costs money and Congress should help. Routine tabulation audits in which a sample of ballots are hand-counted and compared to machine counts help to guard against a variety of threats,

including insider threats. Requiring risk-limiting audits in Federal elections has received bipartisan support in the past.

Our election infrastructure is strong, but it is facing a growing anti-democracy threat from within. Congress can lead the way on protecting democracy from that threat by investing in true election integrity measures.

[The prepared statement of Ms. Ramachandran follows:]

PREPARED STATEMENT OF GOWRI RAMACHANDRAN

JANUARY 20, 2022

Chairwoman Clarke, Ranking Member Garbarino, and Members of the committee: Thank you for the opportunity to discuss the security of our Nation's election infrastructure. Despite a global pandemic, the November 2020 election saw historic turnout and was widely considered the most secure in American history.[1] But an anti-democracy movement, fueled by the Big Lie, poses serious threats to the security of elections. Taking these threats seriously means building upon recent improvements to election infrastructure security, such as the increased use of auditable paper ballots and increased information sharing between State and local election officials and the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

The Brennan Center for Justice—a nonpartisan law and policy institute that focuses on democracy and justice—appreciates the opportunity to report on the security of our election infrastructure, threats to that infrastructure, and ways to secure against these dangers. At the Brennan Center, I focus on election security, and I frequently engage with State and local election officials to advocate for and assist with the implementation of election security and resiliency measures.[2]

In my testimony, I will cover 3 topics. First, I will describe what went right in 2020. This included the wide-spread use of auditable paper ballots, cooperation between State and local election officials and CISA, resiliency measures and money from Congress to ensure voters could exercise their rights safely in a pandemic, and the resiliency of voters themselves, who made thoughtful plans to vote safely and securely. This was all followed by routine, statutory tabulation audits in every swing State, finding no discrepancies sufficient to change the outcome of the Presidential election.

Second, I will describe the threats that the election sabotage movement is posing to election infrastructure. These threats include sham partisan reviews that undermine confidence and security,[3] violent threats and intimidation of election officials and workers,[4] and the potential infiltration of election offices, polling places, and election vendors by anti-democratic forces.[5] Of particular concern: Candidates for

---

[1] U.S. Cybersecurity and Infrastructure Security Agency, "Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees," November 12, 2020, *https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election.*

[2] Reports that I have coauthored include Lawrence Norden, Gowri Ramachandran, and Christopher Deluzio, *A Framework for Election Vendor Oversight,* Brennan Center for Justice, November 12, 2019, *https://www.brennancenter.org/our-work/policy-solutions/framework-election-vendor-oversight;* Gowri Ramachandran and Tim Lau, "How to Keep the 2020 Election Secure," Brennan Center for Justice, June 9, 2020, *https://www.brennancenter.org/our-work/analysis-opinion/how-keep-2020-election-secure;* Edgardo Cortés et al., *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-cyber-attacks-and-technical-problems-during-pandemic-guide;* Jonathan Bydlak et al., *Partisan Election Review Efforts in Five States,* Brennan Center for Justice, July 8, 2021, *https://www.brennancenter.org/our-work/research-reports/partisan-election-review-efforts-five-states;* and Brennan Center for Justice and Bipartisan Policy Center, *Election Officials Under Attack,* June 16, 2021, *https://www.brennancenter.org/our-work/policy-solutions/election-officials-under-attack.*

[3] Gowri Ramachandran, "A Year Later, Sham Election Review Continue to Undermine Democracy," Brennan Center for Justice, January 7, 2022, *https://www.brennancenter.org/our-work/analysis-opinion/year-later-shamelection-reviews-continue-undermine-democracy.*

[4] Brennan Center for Justice and Bipartisan Policy Center, *Election Officials Under Attack;* and Linda So and Jason Szep, "Reuters Unmasks Trump Supporters Who Terrified U.S. Election Officials," Reuters, November 9, 2021, *https://www.reuters.com/investigates/special-report/usa-election-threats/.*

[5] Lawrence Norden and Derek Tisler, "Addressing Insider Threats in Elections," Brennan Center for Justice, December 8, 2021, *https://www.brennancenter.org/our-work/analysis-opinion/addressing-insider-threats-elections.*

election administration positions are raising unprecedented sums as they campaign on election denial.[6]

Third, I will address how election infrastructure can be bolstered against this threat. On-line platforms and traditional media should work with civil society to ensure they are promoting accurate election information.[7] Existing laws against intimidation, coercion, and threats should be enforced,[8] and States should, with support from Congress, consistently adopt traditional guardrails against insider threats. These include restricting and logging access to critical systems, using transparent procedures such as nonpartisan and bipartisan election observation, monitoring for inappropriate activity, requiring vendors to follow cybersecurity, personnel, and supply chain standards, and removing any officials or workers who actively undermine election integrity.[9] Congress should mandate and provide incentives for true election integrity measures, such as risk-limiting audits, rigorous election vendor standards, and independent security testing, as the Freedom to Vote: John R. Lewis Act does.[10]

I. WHAT WENT RIGHT IN 2020

The November 2020 election was the most secure election in American history, with the highest turnout since 1900.[11] This was accomplished through the heroic efforts of State and local election officials, their staff, and pollworkers, with support from CISA, the Election Administration Commission (EAC), Congress, civil society, and voters themselves.

A. An Estimated 96 Percent of Voters Used Voter-Verifiable Paper Ballots

In order to demonstrate the trustworthiness of elections, election officials need auditable, voter-verifiable paper ballot systems.[12] These allow for routine, statutory post-election tabulation audits, in which a sample of paper ballots are compared to the machine-tabulated results. These types of audits are designed to catch tabulation errors, whether they might be the result of malicious activity or technical er-

---

[6] Ian Vandewalker and Lawrence Norden, "Financing of Races for Offices that Oversee Elections: January 2022," Brennan Center for Justice, January 12, 2022, *https://www.brennancenter.org/our-work/research-reports/financing-races-offices-oversee-elections-january-2022.*

[7] Gowri Ramachandran, "Twitter is a Cauldron of Misinformation about the Arizona 2020 Vote Audit," Slate, May 14, 2021, *https://slate.com/technology/2021/05/maricopa-county-arizona-2020-vote-recount-misinformation.html;* and Brennan Center for Justice and Bipartisan Policy Center, *Election Officials Under Attack,* 11.

[8] Linda So and Jason Szep, "Threats of Violence to U.S. Election Officials Highlight Legal Gray Area," September 8, 2021, *https://www.reuters.com/legal/government/threats-violence-us-election-officials-highlight-legal-gray-area-2021-09-08/.*

[9] Elections Project Staff, "Election Observers are Official Actors that Promote Legitimacy and Transparency. They are Typically Appointed, Trained, and are Barred from Voter Intimidation by State and Federal Laws," Bipartisan Policy Center, October 23, 2020, *https://bipartisanpolicy.org/blog/election-observers-are-generally-appointed-and-are-held-to-strict-standards-of-behavior/.*

[10] Freedom to Vote: John R. Lewis Act, H.R. 5746 117th Cong. § 3908, 4001 (2021); Elizabeth Howard, Ronald L. Rivest, and Philip B. Stark, *A Review of Robust Post-Election Audits,* Brennan Center for Justice, November 7, 2019, *https://www.brennancenter.org/our-work/research-reports/review-robust-post-election-audits;* Norden, Ramachandran, and Deluzio, *A Framework for Election Vendor Oversight;* and Cortés et al., *Preparing for Cyberattacks and Technical Problems During the Pandemic: A Guide for Election Officials,* 6.

[11] Women, Asian Americans, and Native Americans were not able to vote in 1900. U.S. Const. amend. XIX (ratified Aug. 18, 1920); Terry Ao Minnis and Mee Moua, "50 Years of the Voting Rights Act: An Asian American Perspective," Asian Americans Advancing Justice, August 4, 2015, *https://advancingjustice-aajc.org/report/50years-voting-rights-act-asian-american-perspective,* ("[U]ntil 1952, Federal policy barred immigrants of Asian descent from becoming U.S. citizens and having access to the vote,"); United States Library of Congress, "Voting Rights for Native Americans," accessed July 25, 2021, *https://www.loc.gov/classroom-materials/elections/right-to-vote/voting-rights-for-native-americans/,* ("The Snyder Act of 1924 admitted Native Americans born in the U.S. to full U.S. citizenship. Though the Fifteenth Amendment, passed in 1870, granted all U.S. citizens the right to vote regardless of race, it wasn't until the Snyder Act that Native Americans could enjoy the rights granted by this amendment,"); Kevin Schaul, Kate Rabinowitz, and Ted Mellnik, "2020 Turnout is the Highest in Over a Century," *Washington Post,* last updated December 28, 2020, *https://www.washingtonpost.com/graphics/2020/elections/voter-turnout/;* and U.S. Cybersecurity and Infrastructure Security Agency, "Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees."

[12] U.S. Election Assistance Commission, Voluntary Voter System Guidelines 2.0, February 10, 2021, 184, 186, *https://www.eac.gov/sites/default/files/TestingCertification/Voluntary_Voting_System_Guidelines_Version_2_0.pdf;* and Kate Polit, "Former CISA Head Krebs Counters GOP Claims, Reassures that 2020 Election was Secure," MeriTalk, December 16, 2020, *https://www.meritalk.com/articles/former-cisa-head-krebs-counters-gop-claims-reassures-that-2020-election-was-secure/.*

rors. When these types of audits are routinely performed by competent administrators in a transparent manner, they can and should boost confidence in the accuracy of electoral outcomes. The Brennan Center and others have long advocated for this type of audit.[13]

In 2016, 1 in 5 voters cast their vote using a paperless voting system that could not be subject to a tabulation audit.[14] But thanks to election officials across the country transitioning to more secure systems that scan paper ballots, as well as the choice of more voters to vote by mail during the pandemic, an estimated 96 percent of voters used voter-verifiable paper ballots in the 2020 election. No swing State used paperless voting machines.[15]

B. CISA and State and Local Election Officials Cooperated To Prevent, Detect, and Recover from Cyber Attacks

CISA established a partnership with and supported State and local election officials in the years and months leading up to the 2020 election by providing vulnerability testing,[16] promoting best practices for resiliency,[17] and providing trainings, such as tabletop exercises[18] in which officials practiced responding to security breaches.

CISA also ramped up its information sharing with State and local election officials, and the public, and this information sharing paid off. For instance, in the fall of 2020, some Florida voters received threatening and intimidating emails in the guise of a far-right group that has promoted violence.[19] The intelligence community detected the true source of the attack, and CISA, the FBI, and the Office of the DNI held a joint press conference to let the public know the truth: That the emails were coming from malicious actors associated with Iran.[20] By quickly informing the public, they were able to reduce any intimidating effect. As Director Ratcliffe stated on October 21, 2020, "These actions are desperate attempts by desperate adversaries . . . We ask every American to do their part to defend against those who wish us harm. The way you do that is quite simple: Do not allow these efforts to have their intended effect. If you receive an intimidating or manipulative email in your inbox, don't be alarmed, and don't spread it."[21]

A few days later, CISA and the FBI issued a public alert, notifying Americans that malicious actors, including some associated with the Iranian government, were

---

[13] Bydlak et al., *Partisan Election Review Efforts in Five States;* U.S. Election Assistance Commission, *Best Practice: Chain of Custody,* July 13, 2021, 15, *https://www.eac.gov/sites/default/files/bestpractices/Chain__of__Custody__Best__Practices.pdf;* and Howard, Rivest, and Stark, *A Review of Robust Post-Election Audits.*

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

[15] Lawrence Norden and Derek Tisler, "Our System is Resilient—but Still has Room for Improvement," Brennan Center for Justice, September 22, 2020, *https://www.brennancenter.org/our-work/research-reports/our-election-system-resilient-still-has-room-improvement.*

[16] U.S. Cybersecurity and Infrastructure Security Agency, Guide to Vulnerability Reporting for America's Election Administrators, last accessed January 13, 2022, 2, *https://www.cisa.gov/sites/default/files/publications/guide-vulnerability-reporting-americas-election-admins__-508.pdf;* and U.S. Cybersecurity and Infrastructure Security Agency, "National Cybersecurity Assessments and Technical Services," last accessed January 13, 2022, *https://www.cisa.gov/uscert/resources/ncats.*

[17] U.S. Cybersecurity and Infrastructure Security Agency, "Election Security—Physical Security of Voting Locations and Election Facilities," last accessed January 13, 2022, *https://www.cisa.gov/sites/default/files/publications/physical-security-of-voting-location-election-facilities__v2__508.pdf;* and U.S. Cybersecurity and Infrastructure Security Agency, "We're in This Together. Mis-, Dis-, and Malinformation Stops with You," last accessed January 13, 2022, *https://www.cisa.gov/sites/default/files/publications/election-disinformation-toolkit__508__0.pdf.*

[18] U.S. Cybersecurity and Infrastructure Security Agency, Elections Cyber Tabletop Exercise Package: Situation Manual, January 2020, *https://www.cisa.gov/sites/default/files/publications/Elections-Cyber-Tabletop-Exercise-Package-20200128-508.pdf;* and Benjamin Freed, "Annual Election Security Tabletop Drill Put Officials through 'Armageddon-Like' Test," StateScoop, July 31, 2020, *https://Statescoop.com/dhs-election-tabletop-exercise-2020/.*

[19] Ellen Nakashima, Amy Gardner, Isaac Stanley-Becker, and Craig Timberg, "U.S. Government Concludes Iran was Behind Threatening Emails Sent to Democrats," *Washington Post,* October 22, 2020, *https://www.washingtonpost.com/technology/2020/10/20/proud-boys-emails-florida/.*

[20] Office of the Director of National Intelligence, "DNI John Ratcliffe's Remarks at Press Conference on Election Security," press release, October 22, 2020, *https://www.dni.gov/index.php/newsroom/press-releases/item/2162-dnijohn-ratcliffe-s-remarks-at-press-conference-on-election-security.*

[21] Office of the Director of National Intelligence, "DNI John Ratcliffe's Remarks at Press Conference on Election Security."

scanning multiple States' election webpages for vulnerabilities, and that one State's voter registration data had successfully been accessed.[22] Shortly thereafter, Florida closed down its State-wide page with a voter information look-up tool and informed voter advocates who objected that the closure was due to a security vulnerability. Advocates were able to secure modifications to the page that did not re-open the security vulnerability, but ensured voters with questions could still obtain the information they needed, such as their polling place location.[23]

C. Resiliency Measures and Money from Congress Helped Americans Vote Safely Despite Pandemic

CISA, election security experts, and voting rights advocates all encouraged the adoption of resiliency measures to help election officials detect, prevent, and importantly, recover from an attack or technical failure.[24] Many election officials employed these measures, including the maintenance of emergency paper ballots, to be used in case ballot marking devices malfunctioned,[25] as well as keeping paper pollbook back-ups in polling places that use electronic pollbooks,[26] in case of a malicious attack or malfunction of the electronic books. Provisional ballots were also kept on hand in case an attack or malfunction prevented pollworkers from confirming a voter's eligibility to vote in real time.[27] Each of these resiliency measures came in handy in at least some locations, helping ensure that voting could continue and voters did not need to be turned away, even when occasional hiccups with equipment occurred.[28]

In addition to these resiliency measures against electronic equipment failures, the provision by many States of multiple options for voting—in-person Election Day, in-person early, and mail voting—served as its own resiliency measure against the pandemic. These options allowed voters to spread themselves out among different voting methods and days, thereby reducing crowds at polling places for the increased safety of all. They also allowed voters to, if faced with a long line due to some technical issue during early voting, return on another day when the problem had been ameliorated.[29] They also meant election officials needed resources—from personal protective equipment for pollworkers and voters voting in person, to extra supplies given uncertainty about which voting methods voters would use and larger

---

[22] U.S. Cybersecurity and Infrastructure Security Agency, "Alert (AA20–304A): Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data," last updated November 3, 2020, *https://www.cisa.gov/uscert/ncas/alerts/aa20-304a.*

[23] Letter from the NAACP Legal Defense Fund et al. to Laurel Lee, Florida Secretary of State, November 1, 2020, *https://www.naacpldf.org/wp-content/uploads/2020.11.01-Letter-re-Voter-Information-Lookup-Tool.pdf;* and NAACP Legal Defense Fund Thurgood Marshall Institute, *Democracy Defended,* September 2, 2021, 74, *https://www.naacpldf.org/wp-content/uploads/LDF__2020__DemocracyDefended-1-3.pdf.*

[24] U.S. Cybersecurity and Infrastructure Security Agency, "#Protect2020," last accessed January 14, 2022, *https://www.cisa.gov/protect2020;* Cortés et al., *Preparing for Cyberattacks and Technical Problems During the Pandemic: A Guide for Election Officials;* and Common Cause, "Common Cause Georgia Urges Secretary Raffensperger to Ensure Georgians Are Not Denied the Right to Vote on November 3," press release, October 1, 2020, *https://www.commoncause.org/press-release/common-cause-georgia-urges-secretary-raffensperger-to-ensure-georgians-are-not-denied-the-right-to-vote-on-november-3/.*

[25] J.D. Capelouto and Ben Brasch, "Voting Machines Finally Working at Fulton Polling Place; Paper Ballots Used," *Atlanta-Journal Constitution,* November 3, 2020, *https://www.ajc.com/news/atlanta-news/voting-machines-down-at-one-fulton-polling-place-paper-ballots-in-use/OC3TGOUEGRDMVFPMZ6X7ONLMNA/;* and Michaelle Bond, Julia Terruso, and Justine McDaniel, "Philly Polling Locations Got the Wrong Voting Machines, Causing Confusion and Long Lines: 'It was a Mess,'" *Philadelphia Inquirer,* June 2, 2020, *https://www.inquirer.com/politics/election/live/pa-2020-primary-election-philadelphia-live-updates-results20200602.html.*

[26] Rick Rouan, "Election Day: Some Voters See Delays at Polls as Franklin County Switches to Paper Pollbooks," *Columbus Dispatch,* November 3, 2020, *https://www.dispatch.com/story/news/politics/elections/2020/11/03/franklin-county-shifts-paper-pollbooks-after-data-upload-problem/6135788002/;* see also Michigan Election Security Advisory Commission, *Report and Recommendations,* Michigan Secretary of State, October 2020, 14, *https://www.michigan.gov/documents/sos/ESAC__Report__Recommendations__706522__7.pdf.*

[27] Ben Finley, Alan Suderman, and Denise LaVoie, "Cut Cable Shuts Down Virginia Voter Portal; Lawsuit Filed," Associated Press, October 13, 2020, *https://apnews.com/article/election-2020-us-news-ap-top-news-media-socialmedia-f6525ef6254a940c91b98d2668c43892/.*

[28] Andrea Córdova McCadney, Derek Tisler, and Lawrence Norden, "2020's Lessons for Election Security," December 16, 2020, *https://www.brennancenter.org/our-work/research-reports/2020's-lessons-election-security.*

[29] Córdova, McCadney, Tisler, and Norden, "2020's Lessons for Election Security."

facilities for workers to socially distance in while processing and tabulating mail ballots.[30]

The resiliency measures that election officials employed and the money that Congress provided to help pay for them was crucial in running a safe and secure election.[31]

D. Legitimate Post-Election Audits and Recounts Confirmed that Outcomes Were Correct

Finally, after Election Day came and went, routine, statutory tabulation audits were performed in every swing State, with additional recounts in some. None found discrepancies that would have been sufficient to alter the outcome of the Presidential election, thereby providing added confidence in the integrity of the election.[32]

Of course, there is room for improvement. Ideally, all States would conduct routine, statutory tabulation audits with the opportunity for nonpartisan and bipartisan observation. In these audits, a sample of ballots would be compared to machine counts, and ideally, they would include risk-limiting audits. In a risk-limiting audit, the number of ballots sampled varies based on how close the contest being audited is, in order to provide a pre-determined statistical level of confidence that any discrepancies were not sufficient to alter the outcome.[33]

Currently, most States have some kind of routine post-election tabulation audit, and only a few States conduct risk-limiting audits.[34] Requiring risk-limiting audits is an example of the kind of measure that could truly improve upon election integrity, as opposed to sham partisan reviews,[35] laws that make it easier for monitors to interfere with and disturb election administration,[36] or laws that make it impossible for election officials to assist and educate voters about their rights.[37]

II. THREAT OF ELECTION SABOTAGE

It is imperative that all those who worked to secure our election infrastructure against the threat of foreign interference and attacks in 2020 continue those efforts. But the events of the past year have shown that there is a fast-growing threat of election sabotage from an anti-democratic movement within our own country, and that this threat also deserves focus. In fact, the two threats could compound each other, with home-grown election conspiracies making it easier for foreign governments and their agents to accelerate destabilization merely by seeding and amplifying doubts and confusion, rather than investing in developing sophisticated cyber attacks.

The domestic anti-democracy movement also threatens election infrastructure directly, through sham partisan reviews that undermine not only confidence but secu-

---

[30] Yelena Dzhanova, "The New Challenge for State Election Officials? How Much Hand Sanitizer is Enough," CNBC, August 10, 2020, *https://www.cnbc.com/2020/08/10/coronavirus-distributing-masks-and-sanitizer-a-challenge-for-2020-election.html;* Tim Harper, Rachel Orey, and Collier Fernekes, *Counting the Vote During the 2020 Election,* Bipartisan Policy Center, August 25, 2020, *https://bipartisanpolicy.org/report/counting-the-vote-during-the-2020-election/;* and Kendall Karson, "'I Don't Think You Really Can' Make the Election Safe: Wisconsin Gears Up for Next Primary Amid Coronavirus," ABC News, March 31, 2020, *https://abcnews.go.com/Politics/make-election-safe-wisconsin-gears-primary-amid-coronavirus/story?id=69879453.*

[31] Córdova McCadney, Tisler, and Norden, "2020's Lessons for Election Security."

[32] Bydlak et al., *Partisan Election Review Efforts in Five States.*

[33] Elizabeth Howard, Turquoise Baker, and Paul Rosenzweig, *Risk-Limiting Audits in Arizona,* Brennan Center for Justice, February 1, 2021, 3–4, *https://www.brennancenter.org/our-work/research-reports/risk-limiting-audits-arizona.*

[34] Derek Tisler, Elizabeth Howard, and Edgardo Cortés, "The Roadmap to the Official Count in an Unprecedented Election," Brennan Center for Justice, October 26, 2020, *https://www.brennancenter.org/our-work/researchreports/roadmap-official-count-unprecedented-election;* National Conference of State Legislatures, "Post-Election Audits," last updated October 25, 2019, *https://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx#State%20reqs;* and National Conference of State Legislatures, "Risk-Limiting Audits," last updated September 16, 2021, *https://www.ncsl.org/research/elections-and-campaigns/risk-limiting-audits.aspx.*

[35] Elizabeth Howard and Gowri Ramachandran, "Partisan Arizona Election 'Audit' Was Flawed from the Start," Brennan Center for Justice, September 27, 2021, *https://www.brennancenter.org/our-work/analysis-opinion/partisan-arizona-election-audit-was-flawed-start.*

[36] Eliza Sweren-Becker, "Who Watches the Poll Watchers?," Brennan Center for Justice, April 29, 2021, *https://www.brennancenter.org/our-work/research-reports/who-watches-poll-watchers.*

[37] Tyler Buchanan, "Some Voter Education Programs May Be in Jeopardy Due to New Ohio Law," Ohio Capital Journal, July 16, 2021, *https://ohiocapitaljournal.com/2021/07/16/some-voter-education-programs-may-be-in-jeopardy-due-to-new-ohio-law/;* and TX S.B. 1 § 4.02 (2021) (omnibus bill with several restrictive provisions).

rity, and through a variety of threats to the integrity of the people who make up our election infrastructure—election officials, election workers, and election vendor personnel.

A. Sham Partisan Reviews Undermine Security

Loyalists of former president Donald Trump invaded the U.S. Capitol 1 year ago, carrying weapons, waving the Confederate flag, and insisting that the 2020 election was fraudulent. There was no credible support for the claims of "Stop the Steal" advocates. Nevertheless, Pro-Trump politicians have spent the past year attempting to fabricate that support. They have dented public confidence in the voting process and made it harder for voters, in particular voters of color, to vote. Less recognized, but no less damaging, is the way they have co-opted and undermined a critical tool of our democracy: The post-election audit.[38]

Many States have rigorous protocols for post-election audits, including randomized selection of the electronic tallies to be checked against paper records, a commitment to objectivity throughout the process, and conducting the audit in full public view.[39] When these standards are upheld, post-election audits help check that the outcomes of elections are accurate, and they maintain or restore public confidence in our democracy. The sham reviews following the 2020 election are, essentially, the opposite of this. They were initiated for partisan reasons, as part of an attempt to overturn the will of the voters.

They can also undermine security by providing unmonitored access to systems to biased partisans,[40] leading to equipment no longer being safe to deploy in future elections. Ballot security breaches are another damaging effect, with inexperienced partisans permitting those handling the ballots to use pens that could change the vote records.[41] They have also threatened potential voter intimidation with plans for biased partisans to knock on voters' doors asking questions.[42] These security problems with partisan reviews are exemplified in the movement's most prominent effort to date: The partisan review[43] of Maricopa County's 2020 election, conducted by the contractor Cyber Ninjas. Cyber Ninjas finally issued a report in September 2021, replacing the outright lies that have triggered defamation lawsuits against other Big Lie proponents with copious and misleading innuendo.[44] The Maricopa County Recorder, Stephen Richer (R), recently issued a lengthy point-by-point rebuttal, in which the county identified 75 claims made by the audit team and debunked them all. The county's analysis determined 38 were inaccurate, 25 were misleading, and 11 were false.[45]

The contractors' most attention-grabbing findings fit the pattern[46] that purveyors of voter fraud myths have long followed: Willful ignorance[47] of basic probability,

---

[38] Brennan Center for Justice, "Post-Election Audits," last accessed January 14, 2022, *https://www.brennancenter.org/issues/defend-our-elections/election-security/post-election-audits.*

[39] National Conference of State Legislatures, "Post-Election Audits"; and Howard, Rivest, and Stark, *A Review of Robust Post-Election Audits.*

[40] Katie Hobbs to Maricopa County Board of Supervisors, May 20, 2021, *https://s3.documentcloud.org/documents/20784519/hobbs-letter-to-maricopa-supervisors-5-20-21.pdf;* and Jeremy Duda, "Wake Technology Services Audited a Pennsylvania Election as part of the#StopTheSteal Movement," *Arizona Mirror,* May 21, 2021, *https://www.azmirror.com/2021/05/21/wake-technology-services-audited-a-pennsylvania-election-as-part-of-the-stop-the-steal-movement/.*

[41] Felicia Sonmez and Rosalind S. Helderman, "Observers of Arizona's GOP-Led Election Audit Document Security Breaches, Prohibited Items on Counting floor," *Washington Post,* June 2, 2021, *https://www.washingtonpost.com/politics/trump-election-arizona-audit/2021/06/02/56de9282-c3af-11eb-9a8df95d7724967c_story.html.*

[42] Pamela S. Karlan to Karen Fann, May 5, 2021, *https://www.justice.gov/crt/case-document/file/1424586/download;* and Fredreka Schouten, "Trump Loyalists are Knocking on Voters' Doors in the Latest Quest to Find Fraud in the 2020 Election," CNN, December 18, 2021, *https://www.cnn.com/2021/12/18/politics/trump-supporters-knock-on-doors-in-search-for-2020-fraud/index.html.*

[43] Bydlak et al., *Partisan Election Review Efforts in Five States.*

[44] Howard and Ramachandran, "Partisan Arizona Election 'Audit' Was Flawed from the Start."

[45] Jeremy Duda, "Maricopa County Rebuts 'Audit' Findings, GOP's Bogus Election Claims," *Arizona Mirror,* January 5, 2022, *https://www.azmirror.com/2022/01/05/maricopa-county-rebuts-audit-findings-bogus-election-claims.*

[46] Brennan Center for Justice, *Analysis of the September 15, 2005 Voter Fraud Report Submitted to the New Jersey Attorney General,* December 2005, 1, *https://www.brennancenter.org/sites/default/files/analysis/Analysis%20of%20the%2091505%20Voter%20Fraud%20Report.pdf.*

[47] Gowri Ramachandran, "The Arizona's Senate's Contractors Fail to Understand Basic Probability and Voter Data," Brennan Center for Justice, October 1, 2021, *https://www.brennancenter.org/our-work/analysis-opinion/arizona-senates-contractors-fail-understand-basic-probability-and-voter.*

common election laws, and routine election administration procedures in order to raise baseless suspicions about fellow voters[48] and the dedicated public servants[49] who count their votes and certify the results. The report claims it is suspicious that some voters share the same full name and birth year—it isn't.[50] It uses a commercial move tracking service to raise suspicions about voters who, according to the commercial service, moved before the election. But even leaving aside the accuracy of the commercial service's data, temporary moves do not alter eligibility to vote in Arizona.[51] Unsurprisingly, the Cyber Ninjas audit was promptly used in the continuing disinformation campaign against our elections, with Trump citing its "critical"—and false—"finding" that 23,344 ballots were somehow impacted by the voters purportedly moving.[52]

The push to conduct partisan reviews continues to spread.[53] State legislators in Pennsylvania have proposed conducting their own partisan review that would use the Arizona Senate's actions as a model. Assembly members in Wisconsin have launched a partisan effort there, targeting[54] officials in its largest cities: Milwaukee, Madison, Racine, Kenosha, and Green Bay. Despite the dismissal of a lawsuit seeking to gain access to ballots in Fulton County, GA, for a partisan review,[55] gubernatorial candidate David Perdue has sued Fulton County officials seeking a review.[56] Now, even in States that President Trump won, such as Texas, Florida, and Idaho, local party activists have demanded these reviews over the objections of local election supervisors of both major parties.[57]

B. Violent Threats and Intimidation, Along with Partisan Attacks, Are Pushing Out Personnel Committed to Free and Fair Elections

The Brennan Center for Justice commissioned a national survey of election officials this spring, which found that roughly 1 in 3 election officials feel unsafe because of their job, and approximately 1 in 6 listed threats to their lives as a job-

---

[48] Brennan Center for Justice to Cobb County Board of Elections and Registration, December 18, 2020, *https://www.brennancenter.org/sites/default/files/202012/2020.12.18%20-Brennan%20Center%20Letter%20to%20Cobb%20County%20Board%20of%20Elections.pdf.*

[49] Reuters Staff, "Fact Check: Massachusetts Election Officials Have Not Destroyed Ballots or Committed Election Fraud," Reuters, October 2, 2020, *https://www.reuters.com/article/uk-factcheck-election-ballot-massachuset/factcheck-massachusetts-election-officials-have-not-destroyed-ballots-or-committed-election-fraud-idUSKBN26N2AF.*

[50] Ramachandran, "The Arizona's Senate's Contractors Fail to Understand Basic Probability and Voter Data."

[51] Howard and Ramachandran, "Partisan Arizona Election 'Audit' Was Flawed from the Start."

[52] Daniel Funke, "Fact Check: Arizona Audit Affirmed Biden's Win, Didn't Prove Voter Fraud, Contrary to Trump Claim," *USA Today,* September 28, 2021, *https://www.usatoday.com/story/news/factcheck/2021/09/28/fact-check-arizona-audit-affirms-biden-win-doesnt-prove-voter-fraud/5846640001/;* and Maricopa County (@MaricopaCounty), "CLAIM: 23,344 mail-in ballots voted from a prior address. BOTTOM LINE: Cyber Ninjas still don't understand this is legal under Federal election law. To label it a "critical" concern is either intentionally misleading or staggeringly ignorant. AZ senators should know this too," Twitter, September 24, 2021, 2:32 p.m., *https://twitter.com/maricopacounty/status/1441470631787200514.*

[53] Allan Smith, "Not Just Arizona: Republicans Push More Partisan Election 'Audits,'" NBC News, June 4, 2021, *https://www.nbcnews.com/politics/donald-trump/not-just-arizona-republicans-push-more-partisan-election-auditsn1268644.*

[54] Christine Hatfield, "Election Officials Across Wisconsin Receive Subpoenas in GOP 2020 Election Probe," Wisconsin Public Radio, October 1, 2021, *https://www.wpr.org/election-officials-across-wisconsin-receive-subpoenas-gop-2020-election-probe.*

[55] Nicholas Reimann, "Georgia Judge Dismisses Lawsuit Seeking Election Audit," *Forbes,* October 13, 2021, *https://www.forbes.com/sites/nicholasreimann/2021/10/13/georgia-judge-dismisses-lawsuit-seeking-electionaudit/?sh=3e4f2df3107f.*

[56] Mark Niesse, "Perdue Sues to Inspect Absentee Ballots From 2020 Georgia Election," *Atlanta Journal-Constitution,* December 10, 2021, *https://www.ajc.com/politics/perdue-sues-to-inspect-absentee-ballots-from-2020georgia-election/ERS26VWUQ5AZRAFRCLBPMFINUY/.*

[57] Alexa Ura and Allyson Waller, "First Part of Texas' 2020 Election Audit Reveals Few Issues, Echoes Findings From Review Processes Already in Place," *Texas Tribune,* December 31, 2021, *https://www.texastribune.org/2021/12/31/secretary-state-texas-election-audit/;* Mitch Perry, "DeSantis Appointee Dismisses Election 'Forensic Audit' For Hillsborough, Orange, 3 Other Counties," *Spectrum News: Bay News 9,* July 28, 2021, *https://www.baynews9.com/fl/tampa/news/2021/07/28/there-will-be-no-audits-of-florida-s-election-says-sec-of-state?web=1-&wdLOR=cAFEC4A74-114C-47B8-9D94-A1FC306B6BED;* Idaho Secretary of State, "Idaho Declares 'Big Lie' Allegations 'Without Merit,' Confirms Idaho Election Integrity," October 6, 2021, *https://sos.idaho.gov/2021/10/06/idaho-declares-big-lie-allegations-without-merit-confirms-idaho-election-integrity;* and Lawrence Mower, "'Tone Down the Rhetoric': Florida Election Officials Tell Politicians to Chill Out," *Tampa Bay Times,* October 21, 2021, *https://www.tampabay.com/news/florida-politics/2021/10/21/tone-down-the-rhetoric-florida-elections-officials-tell-politicians-to-chill-out/.*

related concern.[58] This is unacceptable in a functioning democracy. The people who risked their lives during a pandemic to ensure that all eligible voters could vote, that they could vote safely, and that their votes would be counted accurately, cannot be subject to attacks and intimidation. Not only do they deserve better, but our democracy cannot survive when dedicated, honest people who provided the most secure election in American history, with the highest turnout since 1900 are subjected to death threats, simply for doing their jobs well.[59]

The Department of Justice has created a task force to address the situation, but the overall lack of accountability for these bad actors continues to be dispiriting for the public servants who make our democracy function,[60] and the impetus to step down is strong.[61] In one recent example, despite having the support of at least one Republican Board of Elections member, Jeannetta Watson, the first Black elections director in Macon-Bibb County, Georgia, stepped down last week.[62] Board of Elections member Mike Kaplan said it was "a sad day for our country and especially Macon-Bibb," as he "traced Watson's troubles back to allegations of improper vote counting during the Presidential election. Kaplan said workers were 'followed home every night' and under round-the-clock surveillance. 'The stress and fear is too much,' Kaplan said, adding that he believes Watson went through 'a very contentious election where she was in fear of her life.' "[63]

As one might expect, partisan attacks compound the many other pressures that election officials committed to nonpartisan election administration face, and many are being pushed out or resigning in the face of this pressure.[64] Others are being stripped of their powers by partisan actors, in retaliation for certifying election results, or simply for being the face of nonpartisan election administration.[65]

---

[58] Thirty-two percent of election officials surveyed said that they felt unsafe because of their job. Seventeen percent of local election officials surveyed said that they had been threatened because of their job. Benenson Strategy Group, "The Brennan Center for Justice: Local Election Officials Survey," April 7, 2021, *https://www.brennancenter.org/our-work/research-reports/local-election-officials-survey.*

[59] Women, Asian Americans, and Native Americans were not able to vote in 1900. U.S. Const. amend. XIX (ratified Aug. 18, 1920); Minnis and Moua, "50 Years of the Voting Rights Act: An Asian American Perspective"; United States Library of Congress, "Voting Rights for Native Americans"; Schaul, Rabinowitz, and Mellnik, "2020 Turnout is the Highest in Over a Century"; and U.S. Cybersecurity and Infrastructure Security Agency, "Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees."

[60] So and Szep, "Reuters Unmasks Trump Supporters Who Terrified U.S. Election Officials"; and U.S. Department of Justice, "Justice Department Launches Task Force to Combat Threats Against Election Workers," July 29, 2021, *https://www.justice.gov/opa/blog/justice-department-launches-task-force-combat-threats-against-election-workers-0.*

[61] Tom Barton, "Scott County Auditor Cites Lack of Supervisor Support in Announcing Early Retirement," Quad-City Times, March 10, 2021, *https://qctimes.com/news/local/scott-county-auditor-cites-lack-of-supervisor-support-in-announcing-early-retirement/article_1d6e9afb-9f10-5e97-9037-7cc4a42516e6.html;* Andy Kroll, "They Helped Save Democracy—and Are Being Tormented for It," *Rolling Stone,* January 6, 2022, *https://www.rollingstone.com/politics/politics-features/jan6-election-workers-trump-biden-2020-democracy1279027/;* John Myers, "California's Elections Official Exodus," *Los Angeles Times,* April 12, 2021, *https://www.latimes.com/politics/newsletter/2021-04-12/california-elections-officials-exodus-essential-politics;* Fredreka Schouten and Kelly Mena, "High-Profile Elections Officials Leave Posts After a Tumultuous 2020," *CNN,* February 19, 2021, *https://www.cnn.com/2021/02/19/politics/election-officials-lose-and-leave-jobs/index.html;* Marie Albiges and Tom Lisi, "Pa. Election Officials are Burnt Out and Leaving Their Jobs After 2020 'Nightmare,'" *Spotlight PA,* December 21, 2020, *https://www.spotlightpa.org/news/2020/12/pennsylvania-election-2020-officials-retiring-nightmare/;* and Michael Wines, "After a Nightmare Year, Election Officials Are Quitting," *New York Times,* July 2, 2021, *https://www.nytimes.com/2021/07/02/us/politics/2020-election-voting-officials.html.*

[62] Liz Fabian, "Macon-Bibb Elections Supervisor Resigns, Cites Stress, Workload, New Election Laws," Georgia Public Broadcasting, January 10, 2022, *https://www.gpb.org/news/2022/01/10/macon-bibb-elections-supervisor-resigns-cites-stress-workload-new-election-laws.*

[63] Fabian, "Macon-Bibb Elections Supervisor Resigns, Cites Stress, Workload, New Election Laws."

[64] Wines, "After a Nightmare Year, Election Officials Are Quitting."

[65] Michael Wines, "In Arizona, GOP Lawmakers Strip Power from a Democrat," *New York Times,* June 25, 2021, *https://www.nytimes.com/2021/06/25/us/Arizona-Republicans-voting.html;* Jeremy Schwartz, "Trump Won the County in a Landslide. His Supporters Still Hounded the Elections Administrator Until She Resigned," *ProPublica,* October 12, 2021, *https://www.propublica.org/article/trump-won-the-county-in-a-landslide-his-supporters-still-hounded-the-elections-administrator-until-she-resigned;* Laurel White, "'Partisan Politics at Its Worst': Wisconsin Elections Head Meagan Wolfe Refuses to Step Down," Wisconsin Public Radio, November 1, 2021, *https://www.wpr.org/partisan-politics-its-worst-wisconsin-elections-head-meagan-wolfe-refuses-step-down;* and Stephen Fowler, "State Election Board Meets for First

Continued

These attacks on election officials are a threat to the security of our election infrastructure, as officials who are committed to conducting free elections and respecting the will of the voters are themselves a crucial element of that infrastructure.

C. Elections Personnel Who Buy Into Conspiracies May Pose an Insider Threat

Unfortunately, almost one-third of Americans still believe the false narrative that the 2020 election was stolen, "a number that has not budged across five polls in which Monmouth [University Polling Institute] asked this question during the past year."[66] Given this fact, we shouldn't be shocked that among the more than 8,000 local election officials[67]—and tens of thousands of additional public and private-sector employees that support their work—there are some who will also buy into these conspiracy theories. In fact, there has been an active effort to recruit and convince[68] election officials to facilitate these conspiracy theories and push the goals of election deniers. There is reason to worry these efforts could gain traction and followers in the election official community, posing yet another threat to the integrity of the human component of our election infrastructure. Those who work for election vendors may also be at risk.[69]

Officials who have promoted election denialism may be especially susceptible to entreaties that they give unauthorized access. We are witnessing the first glimpses now. In Colorado, a county clerk with connections to election conspiracy theorists gave unauthorized access to the county's Dominion voting systems—a vendor targeted by many proponents of the Big Lie.[70] This access allowed the unauthorized person to take photos of passwords for the voting machine software, which then ended up on-line. The secretary of state decertified the county's voting equipment and ordered the county to replace the machines before the next election.[71]

In Michigan, a town clerk who shared election conspiracies on social media and who took office in 2021 refused to allow a vendor to perform routine maintenance on a voting machine because the clerk falsely believed the maintenance would erase old data that could prove the machines were rigged.[72] When a central component of that machine went missing, the State police opened a criminal investigation into the clerk to locate the since-found equipment and determine whether the equipment had been tampered with.[73]

Time Since Raffensperger Stripped as Chair," Georgia Public Radio, April 29, 2021, *https://www.gpb.org/news/2021/04/29/state-election-board-meets-for-first-time-raffensperger-stripped-chair.*

[66] Monmouth University Polling Institute, "Doubt in American System Increases," November 15, 2021, *https://www.monmouth.edu/polling-institute/reports/monmouthpoll_us_111521/;* and Chris Cillizza, "1 in 3 Americans Believe the 'Big Lie,'" CNN, June 21, 2021, *https://www.cnn.com/2021/06/21/politics/biden-voter-fraud-big-lie-monmouth-poll/index.html.*

[67] Paul Gronke, et al., "Amplifying the Perspectives of Officials at the Front Lines of Elections," Democracy Fund, April 19, 2021, *https://democracyfund.org/idea/amplifying-the-perspectives-of-officials-at-the-front-lines-of-elections/.*

[68] Amy Gardner, Emma Brown, and Devlin Barrett, "Attempted Breach of Ohio County Election Network Draws FBI and State Scrutiny," *Washington Post,* November 19, 2021, *https://www.washingtonpost.com/politics/attempted-breach-ohio-election/2021/11/19/12417a4c-488c-11ec-b8d9232f4afe4d9b_story.html.*

[69] Norden, Ramachandran, and Deluzio, *A Framework for Election Vendor Oversight.*

[70] Bente Birkeland, "After Data is Posted on Conspiracy Site, Colorado County's Voting Machines are Banned," National Public Radio, August 12, 2021, *https://www.npr.org/2021/08/12/1027225157/after-data-is-posted-on-conspiracy-website-colo-countys-voting-machines-are-bann;* Elise Viebeck, "Trump Campaign Debunked Dominion Conspiracy Theories, Internal Memo Shows, Days Before Backers Kept Spreading Them," *Washington Post,* September 22, 2021, *https://www.washingtonpost.com/politics/2021/09/22/trump-dominion-giuliani-powell-memo/.*

[71] Justin Wingerter, "Mesa County Must Replace Election Equipment Due to Security Breach, Secretary of State Says," *Denver Post,* August 21, 2021, *https://www.denverpost.com/2021/08/12/election-security-colorado-mesa-county-jena-griswold/;* and Faith Miller, "Mesa County Commissioners Vote to Replace Dominion Voting Equipment," *Colorado Newsline,* August 24, 2021, *https://coloradonewsline.com/briefs/mesa-county-commissioners-vote-to-replace-dominion-voting-equipment/.*

[72] Jonathan Oosting, "Clerk Decries 'Tyranny' After Michigan Strips Her of Running Election," *Bridge Michigan,* October 27, 2021, *https://www.bridgemi.com/michigan-government/clerk-decries-tyranny-after-michigan-strips-her-running-election;* Jonathan Oosting, "Voting Machine Missing after Michigan Clerk Stripped of Election Power," *Bridge Michigan,* October 28, 2021, *https://www.bridgemi.com/michigan-government/voting-machine-missing-after-michigan-clerk-stripped-election-power;* and Secretary of State Jocelyn Benson to Adams Township Clerk Stephanie Scott, October 25, 2021, *https://content.govdelivery.com/attachments/MISOS/2021/10/25/file_attachments/1976229/Letters%20to%20Adams%20Township%20Clerk.pdf.*

[73] Oosting, "Voting Machine Missing After Michigan Clerk Stripped of Election Power"; and John Tunison, "Missing Hillsdale County Voting Equipment Found, State Checking Whether Tampering Occurred," *Michigan Live,* October 29, 2021, *https://www.mlive.com/news/ann-*

In Ohio, an individual inside a county commissioner's office connected a private laptop to the county network in an attempted breach that State officials believe a government employee may have facilitated.[74] While the connection did not allow access to voting systems, and no sensitive data appears to have been obtained, network traffic captured by the laptop was nonetheless shared at a conference hosted by election conspiracist Mike Lindell—the same conference where information from the Colorado breach was released. Officials in both counties had previously discussed baseless claims about the 2020 election with associates of Lindell.[75]

D. Candidates Are Running for Election Administration Positions with Big Lie Messaging

The magnitude of the insider threat that anti-democracy forces could pose is clarified by examining races for Governor, secretary of state, and local election administrator positions. There are thousands of local election jurisdictions in the United States, and in the vast majority of them, an elected individual is in charge.[76] In past years, the question of who ran and certified our elections has traditionally been of little interest to most. But now, there is an alarming trend of candidates running on (and against) "election denialism."[77]

A preliminary Brennan Center analysis of campaign finance disclosures and messaging by candidates in swing States has found that much of the political discussion this year, 2022, is shaping up to be about 2020 and 2024: Specifically, the Big Lie that the election was "stolen" from former President Trump in 2020, and that if he runs again and loses in 2024, those election results should be overturned.

So far, across 3 States with data available, fundraising in secretary of state races is 2½ times higher than it was by the same point in either of the last two election cycles. And campaigns are making election denial—and opposition to it—a key campaign issue in all 6 of the battleground States with elections for secretary of state in 2022—Arizona,[78] Georgia,[79] Michigan,[80] Minnesota,[81] Nevada,[82] and Wisconsin.[83]

In the contest for Georgia secretary of state, 4 candidates have each raised more than the 2018 winner had at this point, and the candidate raising the most money has refused to acknowledge that Joe Biden won the 2020 election. The Georgia election also features an early indication that these contests are being nationalized. The portion of funding in the race from out-of-state donors so far, 22 percent, is a

---

arbor/2021/10/missing-hillsdale-county-voting-equipment-found-state-checking-whether-tampering-occurred.html.

[74] Lauren Aratani, "FBI Investigates Attempted Breach of Local Election Network in Ohio," Guardian, November 20, 2021, *https://www.theguardian.com/us-news/2021/nov/20/fbi-investigates-attempted-breach-local-election-network-ohio;* and Gardner, Brown, and Barrett, "Attempted Breach of Ohio County Election Network Draws FBI and State Scrutiny."

[75] Gardner, Brown, and Barrett, "Attempted Breach of Ohio County Election Network Draws FBI and State Scrutiny."

[76] Gronke, et al., "Amplifying the Perspectives of Officials at the Front Lines of Elections"; and David C. Kimball and Martha Kropf, "The Street-Level Bureaucrats of Elections: Selection Methods for Local Election Officials," Review of Policy Research 23 (2006): 1257–1268, *https://editions.lib.umn.edu/wpcontent/uploads/sites/3/2016/02/Kimball.Kropf__.Street.Level__.Bureaucrats.of__.Elections.pdf.*

[77] Vandewalker and Norden, "Financing of Races for Offices that Oversee Elections: January 2022."

[78] Mary Jo Pitzl, "Mark Finchem, Election Conspiracy Promoter, Gets Trump's Endorsement for Secretary of State," *Arizona Republic,* September 13, 2021, *https://www.azcentral.com/story/news/politics/elections/2021/09/13/trump-endorses-mark-finchem-arizona-secretary-state-election/8322839002/.*

[79] Jeremy Herb and Fredreka Schouten, "'We Won': Trump and His Allies Barrel Ahead with Election Lies Despite Arizona Review Confirming His Loss," *CNN,* September 27, 2021, *https://www.cnn.com/2021/09/27/politics/arizona-trump-election-lies/index.html.*

[80] Jeremy Herb and Sara Murra, "Trump-Backed Michigan Secretary of State Candidate Spread False Election Claims and January 6 Conspiracy Theories," *CNN,* November 16, 2021, *https://www.cnn.com/2021/11/16/politics/kristina-karamo-michigan-secretary-of-state-candidate/index.html.*

[81] Miles Parks, "Here's Where Election-Denying Candidates are Running to Control Voting," National Public Radio, January 4, 2022, *https://www.npr.org/2022/01/04/1069232219/heres-where-election-deniers-and-doubters-are-running-to-control-voting.*

[82] Tim Reid, Nathan Layne, and Jason Lange, "Special Report: Backers of Trump's False Fraud Claims Seek to Control Next Elections," *Reuters,* September 22, 2021, *https://www.reuters.com/world/us/backers-trumps-false-fraud-claims-seek-control-next-us-elections-2021-09-22/.*

[83] Vandewalker and Norden, "Financing of Races for Offices that Oversee Elections: January 2022."

marked increase over 2018, when it was 13 percent, and more than 4 times the amount from 2014, which was only 5 percent.[84]

In Michigan, the incumbent has raised $1.2 million—6 times what the last incumbent had raised at this point in 2014. This candidate is running against election denialism, against an opponent who has said voting machines in the State could have flipped 200,000 votes to Joe Biden.[85]

Regardless of who enjoys a fundraising advantage in any particular State, voters are likely to be exposed to unprecedented amounts of political spending on the issue of election denialism, with it no longer being taken as a given that elections will be administered in a nonpartisan manner, regardless of the identity of the administrator.

III. WHAT CAN BE DONE

Lawmakers should support the excellent work that CISA, the EAC, and State and local election officials have done to further election integrity. But they should also act now to further mitigate these growing security risks posed by domestic anti-democracy forces. There are a variety of broadly-accepted methods for mitigating insider threats, which State and local jurisdictions should adopt, and on which Congress can lead by providing the needed financial support. Congress can also provide support for the physical safety and security of elections personnel and elections offices, as well as for risk-limiting audits—a true election integrity measure. Others can do their part as well: On-line media platforms and traditional media can work with civil society to ensure they are promoting the most accurate information, and law enforcement at all levels of government can take threats against election administration seriously, enforcing the laws that exist to deter these crimes.

A. Congress Should Provide Support for Mitigating Insider Threats, Including Against Vendors

Insider threat risks have been a central focus of security efforts in other sectors, and best practices, such as those from the Cybersecurity and Infrastructure Security Agency, exist to prevent and respond to this activity.[86]

Among other things that can be done to both secure election systems from insider threats and build public confidence that those systems can be trusted, States and counties should take the following actions, and Congress should provide resources to support these mandates, many of which require financial resources to implement consistently.

1. Restrict access to election systems.

Election officials should ensure that an individual only have access to critical systems—both physical and digital—if access is necessary for that individual to perform their official responsibilities, and only to the extent that those responsibilities require it (this is known as the "principle of least privilege"[87]). In addition, election officials should require all individuals that access critical systems to first complete a background check. A recent regulation in Colorado,[88] for example, restricts voting system access to individuals who have passed a background check and are employees of the county clerk, voting system provider, or secretary of state's office.

Where possible, official procedures should require two people and/or bipartisan teams to be present when accessing election systems, ballots, and election records. Election staff should also be on-site with private vendors at all times.[89]

2. Establish transparent procedures and monitor for inappropriate activity.

Transparency protocols helped officials in Colorado identify the source of leaked voting system information.[90] A State investigation found that the county clerk gave

---

[84] Vandewalker and Norden, "Financing of Races for Offices that Oversee Elections: January 2022."

[85] Vandewalker and Norden, "Financing of Races for Offices that Oversee Elections: January 2022."

[86] U.S. Cybersecurity and Infrastructure Security Agency, "Insider Threat Mitigation," last updated January 6, 2022, *https://www.cisa.gov/insider-threat-mitigation.*

[87] Center for Internet Security, "Election Security Spotlight—Principle of Least Privilege," last accessed January 13, 2022, *https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-principle-of-least-privilege/*.

[88] Office of the Colorado Secretary of State, "Notice of Temporary Adoption," June 17, 2021, *https://www.sos.state.co.us/pubs/rule__making/files/2021/20210617ElectionsNoticeTempAdoption.pdf.*

[89] Norden and Tisler, "Addressing Insider Threats in Elections."

[90] Emma Brown, "An Elections Supervisor Embraced Conspiracy Theories. Officials Say She Has Become an Insider Threat," September 26, 2021, *https://www.washingtonpost.com/inves-*

an unauthorized person a key card, and this card was logged when the individual entered the election facility. The clerk had also blatantly flouted another transparency measure by turning off video surveillance of the voting machines before the breach. But if the information obtained from the breach had not been discussed so publicly, it's possible the State would have missed this activity.

Election officials must adopt and actively review transparency protocols to ensure that every person who accesses election systems is authorized to do so. Funding should be provided for election officials to install key card access to facilities that hold voting systems, so that a log of every entry can be created. All election offices should be equipped with and require 24-hour surveillance of voting systems and ballots, that can be reviewed and compared with access logs in the event of unauthorized activity. Where possible, that footage should be stored for at least 2 years. Both the access logs and surveillance data should be made available to the State, and State officials should ensure that local offices have sufficient procedures in place to detect unauthorized access.

3. Remove and prosecute officials and workers who actively undermine election integrity.

When officials do discover wrongdoing, these individuals must be held accountable. States have different processes for removing election officials. In some cases, the entity that appointed an election official may simply fire that individual. In others, State officials may hold power to remove election administrators or strip them of election responsibilities.[91] Officials may also seek permission from courts to do so.[92] State and local officials, as well as their attorneys, should be familiar with the removal options available and be prepared to take the steps necessary to protect our election infrastructure from insider threats.

Where appropriate, law enforcement officials should also pursue prosecution against election workers who tamper with or allow unauthorized access to voting systems and election materials. State laws may require updating to address this conduct.

4. Increase resiliency against insider threats to vendors.

Private vendors are involved at every stage of an election, from registering voters to counting ballots to reporting results. States can act now to establish standards on cybersecurity, personnel security, and supply chain integrity for their election vendors.[93] Congress should, as the Freedom to Vote: John R. Lewis Act does, directly incentivize vendors to adopt these standards by limiting expenditures of Federal funds to those vendors that conform to best practices, which can be promulgated by CISA.[94]

5. Build in contractual safeguards.

Local election offices can also build in safeguards through contracts when purchasing equipment and services.[95] As a rule, vendors should be held to the same or higher level of standards for access and transparency as county or State employees. This can include background checks and the requirement to always have a State or county employee present when vendors access critical systems. This can also mean restricting or eliminating remote access by vendors.

Some of these solutions require statutory or regulatory changes at the State level, but Congress can take a leading role in providing additional resources for election offices that implementing these changes will necessitate. Congress can also lead on building resiliency of election vendors, at a minimum by limiting the expenditure of Federal funds to those vendors that agree to comply with best practices in security, including resiliency to insider attacks.

B. Congress Should Provide Support for the Security of Election Officials and Workers

Congress should provide resources to States, via the Election Assistance Commission, that can be used for safety training, including prevention and de-escalation

---

tigations/an-elections-supervisor-embraced-conspiracy-theories-officials-say-she-has-become-an-insider-threat/2021/09/26/ee60812e-1a17-11eca99a-5fea2b2da34b_story.html.

[91] Oosting, "Clerk Decries 'Tyranny' After Michigan Strips Her of Running Election."

[92] Colorado Secretary of State, "Mesa County Court Judge Rules in Favor of Removing Peters as Designated Election Official," press release, October 13, 2021, *https://www.sos.state.co.us/pubs/newsRoom/pressReleases/2021/PR20211013Mesa.html.*

[93] Norden, Ramachandran, and Deluzio, *A Framework for Election Vendor Oversight.*

[94] Freedom to Vote: John R. Lewis Act § 3908.

[95] Christopher Deluzio, "A Procurement Guide for Better Election Cybersecurity," Brennan Center for Justice, March 22, 2019, *https://www.brennancenter.org/our-work/policy-solutions/procurement-guide-better-election-cybersecurity.*

training for election workers. Funds could also be provided for education and training for officials on how to protect one's personal information, as well as for States to expand their address protection services to cover election officials and workers. The Freedom To Vote: John R. Lewis Act additionally makes it a crime to reveal the personally identifying information of election officials and pollworkers with the intent to threaten or intimidate them.[96] Resources could also be used to improve the physical security of election offices.[97]

C. Online Platforms and Traditional Media Should Work with Civil Society

The Brennan Center, along with many others, encourages social media and other on-line speech platforms, along with traditional media, to amplify and promote trusted, accurate information about elections.[98] Typically, election officials are and will be trustworthy sources of information about elections. But given the threats to the integrity of election officials posed by candidates who actively promote election disinformation, on-line platforms and traditional media must prepare for the possibility of a high-level election official promoting disinformation. Nonpartisan and bipartisan civil society groups can serve as an additional trusted resource, to help social and traditional media be sure they are promoting the most accurate information.

D. Existing Laws Should Be Enforced

The Department of Justice, and local and State law enforcement and prosecutors, should enforce existing laws against intimidation, coercion, and threats. There must be consequences for attempting to interfere with free and fair elections. The Department of Justice has launched a task force to combat threats against election workers.[99] State and local prosecutors should take these threats seriously as well.

For a recent example of law enforcement bringing charges against someone making threats against an election official, in Genesee County, MI, the chair of the County GOP has recently pled guilty to harassing the Houghton County clerk during her bid for re-election. The clerk initially reported that he called her at 1 a.m., threatening to kill her dogs. The call was traced, a warrant was obtained for his phone records, and eventually he was charged and sentenced to a year of probation, 240 hours of community service, and a $650 fine.[100]

For an example of charges against someone threatening others over their defense of the integrity of the 2020 election, a man in California was recently sentenced to 3 years in prison after sending threatening messages to approximately 50 victims, "targeting those individuals because of their statements expressing that then-President Trump had lost the 2020 Presidential election."[101]

E. Congress Should Promote Legitimate, Risk-Limiting Audits

Another important security measure that guards against a variety of threats, including insider threats, is routine, statutory tabulation audits that include the opportunity for nonpartisan and bipartisan observation. Such audits can provide added confidence that a cyber attack, insider manipulation, or innocent programming error did not corrupt ballot scanners in such a way that the outcome of an election was altered. In particular, risk-limiting audits can provide a consistently high level of statistical confidence in the machine-tabulated outcome of an election contest.

Although at least 24 States as of 2020 had laws requiring routine post-election tabulation audits, only a few States conduct risk-limiting audits.[102] Congress should

---

[96] Freedom to Vote: John R. Lewis Act § 3102.

[97] Brennan Center for Justice and Bipartisan Policy Center, *Election Officials Under Attack,* 4, 6.

[98] Brennan Center for Justice and Bipartisan Policy Center, *Election Officials Under Attack,* 10–15.

[99] U.S. Department of Justice, "Justice Department Launches Task Force to Combat Threats Against Election Workers."

[100] Stephen Borowy, James Felton, and Gray News Staff, "Michigan School Board Member Sentenced to Probation for 'Malicious' Phone Call," WWNY/WNYF, *https://www.wwnytv.com/2022/01/12/michigan-school-board-member-sentenced-probation-malicious-phone-call/*.

[101] U.S. Department of Justice, "California Man Sentenced To 3 Years In Prison For Making Threats Against Political Officials And Journalists Relating To The Outcome Of The 2020 Presidential Election," press release, December 20, 2021, *https://www.justice.gov/usao-sdny/pr/california-man-sentenced-3-years-prison-making-threats-against-political-officials-and.*

[102] Córdova, McCadney, Howard, and Norden, "Voting Machine Security: Where We Stand Six Months Before the New Hampshire Primary"; and National Conference of State Legislatures, "Risk-Limiting Audits."

require—and provide funding for—risk-limiting audits of Federal elections.[103] This would be a positive improvement in election integrity, and it has received bipartisan support in the past.[104]

IV. CONCLUSION

The heroic efforts of many, and in particular State and local election officials committed to free and fair elections, gave us a safe and secure election in November 2020 with historic turnout. Some crucial improvements in security and resiliency had been in the works for a number of years, such as States that transitioned to voting systems that scan paper ballots, or that took advantage of vulnerability assessments provided by CISA. Other resiliency measures had to be implemented in response to the pandemic and benefited from funding provided by Congress. This included increased mail ballot printing to accommodate increased demand from voters, as well as the purchase of secure dropboxes to permit those voters to safely drop off ballots outside. Long-standing best practices, such as the provision of emergency paper ballots, paper pollbook back-ups, and poll workers on standby, took long hours and plenty of financial resources to implement during an extremely high-turnout election with added pandemic-related costs. Carrying out these practices demonstrated a commitment by election officials to ensure eligible voters would not be turned away, even in the case of malfunctioning equipment or a potential cyber attack.

Now, the disinformation campaign that has sowed distrust in that election has seeded an anti-democracy movement that poses significant threats to our election infrastructure. The threats include sham partisan reviews that undermine ballot and election equipment security, while further fueling the disinformation campaign. They also include attacks on election officials and workers that push out and disempower the very people who administered a historically secure election in 2020. And there may be insider threats from those who seek to replace them. Some who are running for election official positions are themselves promoting election conspiracies in their campaigns, highlighting how election officials themselves, election workers, or election vendor personnel can fall victim to and push conspiracies about the 2020 election. These insiders could be susceptible to requests for unauthorized access and other security breaches, as we've seen occur in a few jurisdictions already.

Maintaining a secure election infrastructure will require effort from many parts of society in the weeks and months to come. Congress can lead the way in this effort, by providing resources for States and local jurisdictions to implement measures that protect against insider threats, such as video surveillance of election equipment and background checks for personnel. Congress should also, as the Freedom to Vote: John R. Lewis Act does, incentivize election vendors' adoption of best practices for personnel and supply chain security, by requiring that Federal funds spent on election vendors go to those who agree to abide by these security measures, and by requiring risk-limiting audits in Federal elections. Unlike sham partisan reviews, these would be true election integrity improvements.

Congress should further provide resources for the physical and personal security of election officials, workers, and their offices, while State, local, and Federal law enforcement should treat those who threaten and interfere with fair election administration as the serious threat to democracy that they are. Existing laws must be enforced against these bad actors.

Our election infrastructure is strong, as shown by the 2020 election, but it is facing a growing anti-democracy threat from within. Congress should protect democracy from that threat by investing in true election integrity measures.

Chairwoman CLARKE. I thank you, Ms. Ramachandran, for your testimony. I now recognize Mr. Stamos to summarize his statement for 5 minutes.

---

[103] Freedom to Vote: John R. Lewis Act, § 4001.104 SAFE Act, H.R. 2722, § 121–123, 116th Cong. (2019); and Clerk of the U.S. House of Representatives, "Roll Call 428/Bill Number H.R. 2722," June 27, 2019, *https://clerk.house.gov/Votes/2019428.*

[104] SAFE Act, H.R. 2722, § 121–123, 116th Cong. (2019); and Clerk of the U.S. House of Representatives, "Roll Call 428/Bill Number H.R. 2722," June 27, 2019, *https://clerk.house.gov/Votes/2019428.*

STATEMENT OF ALEX STAMOS, DIRECTOR, STANFORD INTERNET OBSERVATORY, AND COMMISSIONER, ASPEN INSTITUTE COMMISSION ON INFORMATION DISORDER

Mr. STAMOS. Thank you very much, Chairwoman Clarke and Ranking Member Garbarino, for having me here. Ladies and gentlemen, thank you so much for holding this hearing.

It is an honor to be here with these incredible experts in election integrity and infrastructure security. I think my part today is to talk about election disinformation, about the disinformation around elections that can sometimes be tied to attacks against infrastructure, although not necessarily, and especially our findings and what we learned during 2020, and how I think CISA and Congress can react to those things we learned.

In the summer of 2020, we were very fortunate to send a team of interns from Stanford to go work with CISA, as all of you know, the Cybersecurity and Infrastructure Security Agency. Those interns, most of them worked on infrastructure security projects, including Crossfeed which the Ranking Member mentioned. But a couple of them were working on disinformation. One of the experiences they had is that while CISA had really strong authorization capabilities and funding to work on the infrastructure security, a lot of the capability to understand and deal with election disinformation did not exist at the time.

So, as a result, at Stanford we pulled together our friends at the University of Washington, at the Atlantic Council, and a private company called Graphika, and we put together the Election Integrity Partnership. There was about 130 people involved in this project operating throughout the summer and fall and winter of 2020 into early 2021. The goals of the EIP were to identify election misinformation before it went viral, to help create clear and accurate counter-messaging, and then to increase the transparency of what happened during 2020, partially as a reaction to the fact that in 2016, there were a number of disinformation events that we didn't really understand until years later and even don't truly understand now because information was not gathered at the time.

To be clear, the EIP was very tightly scoped. We explicitly did not handle any claims about candidates or arguments about policy, the kind of issues that are core to the democratic process. So, if one candidate said the other candidate was a crook, said something about the other candidate's kids, something like that, that was completely out of scope for us. Our focus was on disinformation around the election itself.

Our 4 areas that we defined was: Procedural interference, this is when you do things like lie about a poll location or say that the election has been canceled to try to get people not to vote; participation interference, which is to try convince people not to vote through disinformation, such as saying warrants are being checked when you vote, you might be arrested at the voting booth; fraud, so content that asked people to do something illegitimate to try to influence the election; and then delegitimization, which is content that delegitimizes the results based upon false or misleading claims.

In the end, EIP had partnerships with civil society, with CISA, the GEC, the Global Engagement Center at the U.S. State Depart-

ment, with major tech platforms, and then with thousands of local election officials via the Multi-State ISAC. If you are interested in our results, they are available in a not very thin volume that I will wave around multiple times today at eipartnership.net. You can get a paper copy there, too. But I will summarize a couple of, I think, the key takeaways of what we learned in 2020.

The first is the disinformation around the election and then disinformation that led to January 6 was first primed by months and months of narrative-building during 2020, mostly, I think, people recognize by allies of President Trump basically saying this election is likely to be stolen. So, the ground was set by months and months of kind-of political messaging that this election is likely to be stolen, you should be on the lookout for anything that indicates that.

This led to what we call both top-down and bottom-up disinformation. So, there is disinformation that was created by elites that then was spread via social media, the normal media, and others. Then there is also disinformation that would come from the grassroots and that would be amplified by the elites. So, you end up with this interesting cycle of kind of the overall guidance of this is what our message is going to be coming from the top, but then a lot of the details being filled in by normal people on social media that amplified the social media.

The vast majority of the election disinformation was from Americans. There were a handful of notable incidents. Ms. Ramachandran mentioned a really important one around Iran. I am sure we will probably talk about that, too. I think that is probably the most interesting one from my perspective, the Iranian involvement. But for the most part, disinformation is an American thing that we are doing to ourselves and doing to each other.

Most of the content that went viral on social media didn't go viral organically or because of algorithms or amplification. It went viral because a small number of verified influencers decided to make it so; that a small number of people that we know exactly who they are, who have hundreds of thousands and millions of followers decided that that was going to be the controversy that day, and they were able to turn that into a viral piece of content. We have a number of examples of that that we can get into if you would like.

One of our findings is that disinformation has become a real multimedia issue. So, the disinformation we are talking about is being spread on social media, but we also see it on AM radio, cable news, podcasts, a variety of different outlets. So, there is not one single place that you can kind-of choke down on this. You have to look at the overall economics of the ecosystem.

Then an interesting finding for us is that live video turned out to be a really big deal, and I am happy to talk more about that.

Chairwoman CLARKE. Well, thank you, Mr. Stamos. I appreciate your testimony. I now recognize Mr. Rosenberg to summarize his statement for 5 minutes.

STATEMENT OF EZRA D. ROSENBERG, CO-DIRECTOR, VOTING RIGHTS PROJECT, LAWYERS' COMMITTEE FOR CIVIL RIGHTS UNDER LAW

Mr. ROSENBERG. Chairwoman Clarke, Ranking Member Garbarino, Members of the subcommittee, thank you very much for giving me the opportunity to testify today regarding threats to election infrastructure and voter confidence. My testimony is going to focus on a second part of the equation, the threat to voter confidence and, in particular, the danger of fabricated claims of lack of voter confidence in our elections being used not to ensure that elections are secure or run with integrity, but as a pretext to suppress the right to vote of millions of voters, predominantly voters of color.

It is important for this subcommittee to distinguish between legitimate, particularized, and supported cybersecurity concerns so as to protect against future and, thankfully as yet, unrealized security threats on the one hand from the unsubstantiated allegations of lack of voter confidence in an otherwise secure system on the other. The former can lead to protections that will continue to make our elections secure. The latter have been used with increasing frequency to make it more difficult for voters to cast their votes and have their votes counted. In considering these issues we urge the subcommittee to not allow the erection of unnecessary obstacles to voting built on the specter of false allegations of fraud and on self-fulfilling prophesies of lack of voter confidence.

Although the right to vote is essential to all Americans, it is perhaps most important to those populations to whom it had been historically denied. As Dr. King put it, it is civil right No. 1. Unfortunately, before the ink was dry on the ratification of the 15th Amendment that guaranteed the right to vote to all Americans regardless of race, there were those who used every means at their disposal to stop Black voters and other voters of color from voting. It took more Constitutional amendments and landmark legislation, like the Voting Rights Act of 1965, to stop practices such as poll taxes and literacy tests and all-White primaries that had prevented voters of color from voting.

The progress gained by these laws was great, but those who wanted to stop voters of color from voting were not deterred. For a few decades, they were severely hampered by Section 5 of the Voting Rights Act, which prevented those jurisdictions with a documented history of discrimination in voting from implementing changes in election practices without preclearance from the attorney general or the court. But Section 5 was effectively gutted by the Supreme Court in its decision in *Shelby County* v. *Holder*.

Now, all this is a preface to what is happening today. Literally from the second Shelby County was handed down, States formally covered under Section 5 have used the supposed lack of voter confidence as justification for the implementation of election practices that make it demonstrably more difficult for voters of color to vote.

First they claim that their new practices are necessary to stop fraud when there were is no evidence of fraud. Indeed, the minute number of alleged fraudulent ballots is far outweighed by the thousands of voters for whom voting is made significantly more burdensome in the name of the fiction of fraud.

Then where they cannot prove fraud they point to public opinion surveys, which they say demonstrate the lack of voter confidence in the system, necessitating stronger protections. But these survey results are themselves the result of the lies, both big and small, spun by those who would use such pretexts to justify their imposing burdens, making it more difficult for certain people, predominantly people of color and lower income people, to vote. This happened in Texas in the failed attempt to implement a discriminatory photo ID law. It is happening today, where spurred by the lies that the 2020 Presidential election was stolen, including bogus claims of voting machine irregularities, laws have been passed in dozens of States making it more difficult for voters of color to vote.

The biggest threat to voter confidence are these lies. Now that every such claim of irregularities in the last Presidential election was rejected by the courts is of little solace. In the legend of the little boy who cried wolf, when real danger came no one came to help him. Here there may be legitimate concerns about the security of our election infrastructure and Congress should be doing everything it can to guard against those dangers where real and substantiated. It should not be led off course by the pernicious lies of the boy who cried wolf and it should not permit the so-called lack of voter confidence fostered by those lies to perpetuate discrimination against voters of color. Thank you.

[The prepared statement of Mr. Rosenberg follows:]

PREPARED STATEMENT OF EZRA D. ROSENBERG

JANUARY 20, 2022

I. INTRODUCTION

Chairwoman Clarke, Ranking Member Garbarino, and Members of the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection & Innovation. My name is Ezra Rosenberg and I am the co-director of the Voting Rights Project of the Lawyers' Committee for Civil Rights Under Law ("Lawyers' Committee"). Thank you for giving me the opportunity to testify today regarding "Securing Democracy: Protecting Against Threats to Election Infrastructure and Voter Confidence."

My testimony will focus on the second part of the equation: The threat to voter confidence, and in particular the danger of fabricated claims of lack of voter confidence in our election results being used as a pretext to suppress the right to vote of millions of voters, predominately voters of color, not to ensure that elections are secure and run with integrity. It is important for this subcommittee to distinguish between legitimate, particularized, and supported cybersecurity concerns so as to protect against future—and, thankfully, as yet unrealized—security threats on the one hand, and blunderbuss and unsubstantiated allegations of lack of voter confidence in an otherwise secure system on the other. The former can and should lead to protections that can continue to make our election infrastructure secure. The latter have been used with increasing frequency to make it more difficult for eligible voters to cast their votes and have their votes counted. In considering these issues, we urge the subcommittee not to conflate the two, and specifically not to allow the erection of unnecessary obstacles to voting built on the specter of false allegations of fraud and on self-fulfilling prophesies of lack of voter confidence.

I come to the views I offer today after having devoted the bulk of the last decade of my career litigating voting rights cases on behalf of voters of color for the Lawyers' Committee. The Lawyers' Committee is a National civil rights organization created at the request of President John F. Kennedy in 1963 to mobilize the private bar to confront issues of racial discrimination pro bono. In fact, I first became associated with the Lawyers' Committee when I was a partner of a large global law firm, and volunteered in 2011 to take on a voting rights case pro bono. That case was the challenge to Texas's strict photo ID law, which I will discuss in my testimony. After I retired from private practice in 2014, the Lawyers' Committee asked

me to join their staff, and since I became co-director of the Voting Rights Project in 2015, I have supervised the filings on behalf of voters and civil rights organizations in over 100 cases dealing with voting rights, many of them with claims brought by persons of color whose ability to vote has been compromised under the guise of insuring voter confidence in election integrity.

The right to vote holds a special place in our democracy. Well over a century ago, in trying to provide an example of the essential truths of this Nation—that a person's life, liberty, or happiness, cannot be subject to arbitrariness and that ours is a Government of laws not of people, the Supreme Court described the "political franchise of voting," as not "strictly . . . a natural right," but "as a fundamental political right, . . . preservative of all rights."[1]

Although the right to vote is essential to all Americans, it has perhaps an even more special place and is of, if possible, even greater importance to people to whom it had been historically denied. As Dr. Martin Luther King called it, it is "Civil Right No. 1."[2] Unfortunately, before the ink was dry on the ratification of the Fifteenth Amendment to the Constitution that guaranteed the right to vote to all citizens, regardless of race or color of their skin, there were those—often in positions of power—who used every means at their disposal to stop Black voters and other voters of color from voting. It took more Constitutional amendments and landmark legislation such as the Voting Rights Act of 1965 (the "Act" or the "VRA"), to stop practices such as poll taxes, literacy tests, all-White primaries, and similar means used to prevent voters of color from voting.

The progress gained by these laws was great. But those who wanted to stop people of color from voting have persevered. For a few decades, they were severely hampered by Section 5 of the Voting Rights Act, which prevented those jurisdictions with a documented history of racial discrimination in voting from implementing any changes in election practices without preclearance from the United States Attorney General or the United States District Court for the District of Columbia. But Section 5 was effectively gutted by the Supreme Court's decision in *Shelby County* v. *Holder*.[3] Additionally, while we have yet to see the full effects of the Supreme Court's more recent decision in *Brnovich* v. *Democratic National Committee,*[4] signs point to that decision's making it unnecessarily more difficult for plaintiffs to prove that a State's election practices result in discrimination against voters of color under Section 2 of the Voting Rights Act. (In recent testimony before the House Judiciary Committee, I discussed these court decisions at greater length.)[5]

All this is a preface to what is happening today. Literally from the second Shelby County was handed down, States formerly covered under Section 5 of the Voting Rights Act have used supposed lack of "voter confidence" as justification for their implementation of election practices that make it demonstrably more difficult for people—predominately people of color—to vote. First, they claim that their new practices are necessary to stop fraud—when there is no evidence of fraud. The number of actual infractions is infinitesimal and not remotely likely to change election outcomes.[6] Indeed, the minute number of alleged fraudulent ballots is far outweighed by the thousands of voters for whom voting is made significantly more burdensome in the name of the fiction of fraud.

Aware they cannot prove fraud, those enacting such laws point to public opinion surveys which, they say, demonstrate lack of voter confidence in the system, necessitating stronger protections. But these survey results, we will show, are the result of the lies—both big and small—spun by those who would use such pretexts to justify their imposing burdens making it more difficult for certain people—predominately people of color and poorer people—to vote. This happened in Texas in the failed attempt to implement a photo ID law that made it more difficult for Black and Latinx voters to vote than for white voters to vote. And it is happening today where, spurred by the lies that the 2020 Presidential election was "stolen" and bogus claims of voting machine irregularities and rogue administrators, laws have

---

[1] *Yick Wo* v. *Hopkins,* 118 U.S. 356, 370 (1886).

[2] Martin Luther King, Jr., *Civil Right No. 1: The Right to Vote,* THE N.Y. TIMES MAG., Mar. 14, 1965, at 26–27, reprinted in A TESTAMENT OF HOPE: THE ESSENTIAL WRITINGS AND SPEECHES OF MARTIN LUTHER KING, JR. 183 (James M. Washington ed., 1991).

[3] 570 U.S. 529 (2013).

[4] U.S. Supreme Court no. 19–1257, decided July 1, 2021.

[5] U.S. HOUSE OF REPRESENTATIVES, COMMITTEE ON THE JUDICIARY, HEARING ON "THE IMPLICATIONS OF *BRNOVICH* V. *DEMOCRATIC NATIONAL COMMITTEE* AND POTENTIAL LEGISLATIVE RESPONSES," JULY 16, 2021.

[6] *The Myth of Voter Fraud,* THE BRENNAN CTR. FOR JUST., *https://www.brennancenter.org/issues/ensure-every-american-can-vote/vote-suppression/myth-voter-fraud.*

been passed in dozens of States making it more difficult for voters of color to vote. The biggest threats to voter confidence are these lies.

That every such claim of irregularities in the last Presidential election was rejected by the courts is of little solace.[7] In the legend of the boy who cried wolf, when real danger came, no one came to help him. Here, there may be legitimate concerns about the security of our election infrastructure, and Congress should be doing everything it can to guard against those dangers, where real and substantiated. It should not be led off-course by the pernicious lies of the boy crying wolf. And it should not permit the so-called lack of voter confidence fostered by those lies to perpetuate discrimination against voters of color.

II. THE USE OF THE FRAUD AND VOTER CONFIDENCE MYTHS TO BURDEN THE RIGHT TO VOTE

As I suggested at the outset, my experience with the Texas voter ID case provides a good example of the use of specious allegations of fraud and lack of voter confidence to justify discriminatory voting practices.

Prior to 2011, Texas had a robust voter identification law, allowing voters to vote upon production of any one of multiple, commonly-held IDs.[8] To the extent that the voter ID requirements were intended to prevent fraud, they seemed to be working quite well. There had been only two convictions for in-person voter impersonation fraud—the only sort of fraud a voter ID requirement addresses—out of 20 million votes cast in Texas between 2001 and 2011.[9]

Nevertheless, in 2011, the Texas legislature passed Senate Bill 14 ("SB 14"), which limited acceptable voter IDs to a handful of photo identification documents, namely a current or not expired for more than 60 days Texas drivers' license or personal identification card issued by the Department of Public Safety, U.S. military card, U.S. passport, Texas license to carry a concealed handgun, or Texas Election Identification Certificate, or a U.S. naturalization paper with a photograph.[10] In the rushed process leading up to the passage of SB 14, the proponents and drafters of SB 14 were repeatedly made aware that, if enacted, the law would have a disproportionate effect on Black and Latinx voters. Nevertheless, they rejected dozens of amendments that would have lessened the impact of the law, and passed SB 14.[11]

SB 14 was found by a three-judge panel of the United States District Court for the District of Columbia to have a retrogressive impact on the rights of Black and Latinx voters in proceedings brought by Texas under Section 5 of the Voting Rights Act, seeking preclearance of the law.[12] While Texas's appeal was pending, the Supreme Court issued its decision in Shelby County holding unconstitutional the coverage formula which defined which jurisdictions were subject to the provisions of Section 5, thus freeing Texas from the requirements of Section 5. That very same afternoon, Texas announced it would start implementing the new photo ID law, forcing the Lawyers' Committee, representing the Texas State Conference of the NAACP and the Mexican American Legislative Caucus of the Texas House of Representatives who had successfully intervened in the Section 5 action, as well as other civil rights organizations and the Department of Justice, to file suit under Section 2 of the Voting Rights Act.

That suit was successful, and Texas was forced to change its law, with the district court ruling—and the Fifth Circuit Court of Appeals affirmance en banc—that Texas's photo ID law discriminated against Black and Latinx voters under the effects prong of Section 2.[13] Specifically, the plaintiffs proved that Black voters were almost twice as likely as White voters, and Latinx voters almost 2 and a half times as likely as White voters, to lack the required IDs, and that Black and Latinx voters were similarly less likely than White voters to be able to obtain the required IDs.[14] As a result of these findings, the court entered an interim remedial order allowing any voter who lacked the required ID to vote upon execution of a declaration of a reasonable impediment. Ultimately, the Texas legislature replaced SB 14 with SB

---

[7] Jim Rutenberg et al., *Trump's Failed Crusade Debunks G.O.P.'s Case for Voting Restrictions: Over and Over, Courts Find No Fraud, but Efforts to Limit Rights Persist,* N.Y. TIMES, Dec. 27, 2020, *https://static01.nyt.com/images/2020/12/27/nytfrontpage/scan.pdf.*

[8] *Veasey* v. *Abbott,* 830 F.3d 216, 225 (5th Cir. 2016) (en banc).

[9] Id. at 238–39.

[10] Id. at 225.

[11] Id. at 236, 239.

[12] *Texas* v. *Holder,* 888 F.Supp.2d 113 (D.D.C. 2012).

[13] *Veasey* v. *Abbott,* 830 F.3d 216.

[14] Id. at 251.

5, which largely tracked the interim remedial order, and the Fifth Circuit Court of Appeals ruled that this provided the plaintiffs with their full remedy.[15]

For present purposes, however, it is the findings of the tenuousness of the justifications provided by the proponents of SB 14—findings that the Fifth Circuit Court of Appeals ruled were material support to a finding of discrimination intent—that are of interest. First, the court noted that "Texas has a history of justifying voter suppression efforts such as the poll tax and literacy tests with the race-neutral reason of promoting ballot integrity."[16] The court reasoned that, while the "Legislature is entitled to set whatever priorities it wishes," and that "Ballot integrity is undoubtedly a worthy goal," there was virtually no evidence of in-person voter fraud in Texas.[17] Second, the court highlighted "that many rationales were given for a voter identification law, which shifted as they were challenged or disproven by opponents."[18] The first of these was fraud prevention; the second was that "such laws fostered public confidence in election integrity and increase voter turnout."[19] The district court found that "there was no credible evidence" to support these claim.[20]

III. THE NEXT GENERATION OF FALSE JUSTIFICATIONS: THE ATTACK ON DEMOCRACY

While, as the Fifth Circuit Court of Appeals noted in *Veasey* v. *Abbott,* the use of fraud as justification for voter suppressive laws is not new, the 2020 Presidential election added a new and extraordinarily dangerous twist: Using spurious and unsubstantiated voter fraud allegations—often directed at voting machine technology and other election infrastructure elements—in an attempt to reverse the will of the people altogether. This reached a crescendo in the dozens of suits brought by former President Donald Trump and his allies—many of which we at the Lawyers' Committee participated in, representing the NAACP as an intervenor or amicus curiae, as invariably these suits targeted areas of large numbers of Black voters in places such as Atlanta, Detroit, Milwaukee, and Philadelphia.

A. The 2020 Presidential Election Was Not Perfect, But It Was Secure

During the 2020 Presidential Election, we witnessed the largest voter turnout in American history. 159,633,396 voters turned out in the 2020 election, 20 million more than in any previous election. Turnout was the highest in 120 years in terms of the percentage of voting-eligible population, with 66.7 percent casting ballots. President Joseph Biden became the first U.S. Presidential candidate to receive more than 80 million votes, with a final tally of 81,283,098 votes, or 51.3 percent of all votes cast for President. Former President Trump received the second highest total of any U.S. Presidential candidate, trailing President Biden by a little over 7 million votes.[21]

As a result of the pandemic, an unprecedented number of ballots were cast through early voting or vote-by-mail. Over 101.4 million voters in the Presidential Election cast their ballots before Election Day, nearly two-thirds of all ballots cast. Of those early votes, about 65.6 million were returned via mail-in ballots. Elections security experts lauded the 2020 Presidential Election as the "most secure in American history."[22]

That conclusion was shared by then-President Trump's own appointees. A joint statement issued by the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency, or CISA, concluded:

"The November 3d election was the most secure in American history . . . There is no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised. Other security measures like pre-election testing, State certification of voting equipment, and the U.S. Election Assistance Commission's (EAC) certification of voting equipment help to build additional confidence in the voting systems used in 2020. While we know there are many unfounded claims and opportunities for misinformation about the process of our elections, we can assure you we have the utmost confidence in the security and integrity of our elections, and you

---

[15] *Veasey* v. *Abbott,* 888 F.3d 792 (5th Cir. 2018).
[16] 830 F.3d at 237.
[17] 830 F.3d at 238–39.
[18] 830 F.3d at 240–41.
[19] *Veasey* v. *Perry,* 71 F.Supp. 3d 627, 655 (S.D. Tex. 2014), affirmed in part and reversed in part on other grounds sub nom. *Veasey* v. *Abbott,* 830 F.3d 216 (5th Cir. 2016) (en banc).
[20] Id.
[21] James M. Lindsay, *The 2020 Election by the Numbers,* COUNCIL ON FOREIGN REL., (Dec. 15, 2020), *https://www.cfr.org/blog/2020-election-numbers.*
[22] Sara Cook, *Election infrastructure officials: 2020 election was "most secure in American history" ,* CBS NEWS (Nov. 20, 2020), *https://www.cbsnews.com/live-updates/2020-election-most-secure-history-dhs/.*

should too. When you have questions, turn to elections officials as trusted voices as they administer elections."[23]

This is not to say that the 2020 election—or any election—was perfect. The Lawyers' Committee, which helps coordinate the National, non-partisan Election Protection coalition, including the 866–OUR–VOTE hotline, received numerous reports of voters of color having trouble registering to vote, casting their ballot, or having their ballot counted. A little over 54 percent of all voters who called the Election Protection Hotline and reported their race or ethnicity were voters of color. They reported several basic barriers to voting access, which disproportionately impacted voters of color:

- Restrictions or lack of information about voter registration;
- Lack of notice about the consolidation or closure of polling places;
- Purging of voter rolls in violation of the National Voter Registration Act;
- Lack of information about how to access vote-by-mail opportunities;
- Unreasonable vote-by-mail deadlines, due to mail delivery and return delays;
- Rejection of absentee ballots through misuse of signature-matching procedures;
- Restrictive voter identification laws, which failed to provide alternatives to voters lacking required information (such as those voters with nontraditional mailing addresses) or who do not have reasonable access to Government offices that offer accepted forms of identification; and
- Long lines that resulted in hours-long wait times due to an insufficient number of voting machines or equipment malfunctions.

We also received reports of violations of Federal law, including the failure to provide language assistance in violation of Section 203 of the Voting Rights Act and the denial of assistance from a person chosen by the voter in violation of Section 208 of the Act. Many of these problems were exacerbated by overwhelmed election officials who were unprepared and under-resourced for the unprecedented levels of voter participation, particularly during a pandemic.

B. The "Big Lie" Is Not About Election Infrastructure Security

Thus, particularly in the context of the pandemic, the 2020 election was an unqualified success insofar as ensuring that cast ballots were counted accurately. Nevertheless, lawyers representing the interests of former President Trump filed suit after suit in Arizona, Georgia, Michigan, Pennsylvania, and Wisconsin, alleging that the election was not secure, that it had been "stolen" or "rigged." Often the allegations took the form of attacks on the election infrastructure. These allegations, made in a Michigan suit, are representative:

> 1. "'[T]he absentee voting counts in some counties in Michigan have likely been manipulated by a computer algorithm,' and [] at some time after the 2016 election, software was installed that programmed tabulating machines to 'shift a percentage of absentee ballot votes from Trump to Biden.'"
> 2. "Smartmatic and Dominion were founded by foreign oligarchs and dictators to ensure computerized ballot-stuffing and vote manipulation to whatever level was needed to make certain Venezuelan dictator Hugo Chavez never lost another election."
> 3. "The several spikes cast solely for Biden could easily be produced in the Dominion system by preloading batches of blank ballots in files such as Write-Ins, then casting them all for Biden using the Override Procedure (to cast Write-In ballots) that is available to the operator of the system."[24]

All of these claims and other similar claims were summarily dismissed by court after court—often by judges who had been appointed by President Trump—and some of the attorneys making these claims were ultimately subjected to sanctions and disciplinary proceedings for advancing claims that were not based on facts.[25]

Congress should ensure that electronic voting machines are both secure from interference—domestic or foreign—and provide accessible means for all voters that are

---

[23] Joint Statement from Elections Infrastructure Government Coordinating Council & The Election Infrastructure Sector Coordinating Executive Committees, Nov. 12, 2020, *https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election.*

[24] *Timothy King, et al.* v. *Gretchen Whitmer, et al.*, United States District Court for the Eastern District of Michigan, case no. 2:20–cv–13134–LVP–RSW, ECF. No. 172, Aug. 25, 2021, p. 15 (internal citations omitted).

[25] See generally *Tracking election disputes, lawsuits, and recounts,* BALLOTPEDIA'S 2020 ELECTION HELP DESK, *https://ballotpedia.org;* Jacob Shamsian & Sonam Sheth, *Trump and his allies filed more than 40 lawsuits challenging the 2020 election results. All of them failed,* BUSINESS INSIDER (Feb. 22, 2021), *https://www.businessinsider.com/trump-campaign-lawsuits-election-results-2020-11; Postelection lawsuits related to the 2020 United States Presidential election,* WIKIPEDIA *https://en.wikipedia.org* (last accessed January 17, 2022).

fully auditable, both by election officials to ensure that the votes counted by the machines match the votes cast by the voters and by the voters themselves before they leave the polling places. But it should do so based on sound, substantiated evidence, not political posturing.

For example, the Lawyers' Committee was co-counsel for plaintiffs in a case dealing with cybersecurity issues in Georgia. There, the court described the evidence submitted by plaintiffs as "a mountain of evidence demonstrating the burdens to the voting process and to the casting of a secure, reliable, counted ballot that some portion of voters across Georgia, including Plaintiffs, had experienced as a result of the State's continued use of voting equipment, software, hardware, election and voter databases, that were demonstrably shown to be antiquated, seriously flawed, and vulnerable to failure, breach, contamination and attack."[26] As a result, in April 2019, the court enjoined the use of Georgia's Direct Recording Electronic voting machines (DRE) and Global Election Management Systems (GEMS) beyond the 2019 election cycle. But nowhere in that litigation did the plaintiffs suggest that an election had ever been tampered with. Rather, the focus of the case was on the real vulnerabilities of the system and the need to take reasonable steps to protect against potential threats.

That, unfortunately, is not what the "Big Lie" is all about. It is not tethered to reality, let alone evidence.

C. The "Big Lie's" Intent and Effect is to Undermine Voter Confidence

The "Big Lie" that the 2020 Presidential election was stolen has become the stock in trade of numerous politicians, including the former President, and has become a rallying call for a sector of the electorate. This is not merely a matter of partisan politics. Were it so, the Lawyers' Committee, as a non-partisan organization, would be silent. The sad fact is that the repetition of the "Big Lie" eats at the core of our democracy.

Studies have shown that disinformation campaigns such as the "Big Lie" can have a damaging impact on voters' faith in the system. After President George W. Bush won reelection, Republicans had a high level of confidence in the accuracy of the election, but this figure dropped significantly in the following decade. During that time there was a mix of wins by both parties, but also the beginning of a vigorous campaign by certain political sectors pressing unsubstantiated claims against election systems. As the November 2016 election day approached, then-Presidential candidate Trump increased the volume:

"Of course there is large scale voter fraud happening on and before election day.
"The election is absolutely being rigged by the dishonest and distorted media pushing Crooked Hillary—but also at many polling places—SAD".[27]

One survey of voting age citizens at the time of the 2016 election found that allegations of election rigging changed their belief about whether fraud was likely if the fraud would hurt their political party. An author of the study concluded, "Allegations that the election is rigged reduce Americans' support for the democratic norms that underlie the U.S. system of government."[28]

In a study of former President Trump's claims of election fraud conducted by Brendan Nyhan of Dartmouth and other scholars, researchers found the claims undermined faith in elections, especially among his supporters.[29] Saying that confidence in elections may be a "soft target," Dr. Nyhan commented, "It's complicated, hard to observe, unintuitive, and relies on trust. Trust in institutions seems to be easier to destroy than to build." Speaking of the unsubstantiated claims, he added that his major worry is the damage to "institutional legitimacy."[30]

Dr. Nyhan's fear is well-founded. In 2006, the same year that we saw a strong bipartisan reauthorization of the Voting Rights Act, the United States was ranked

---

[26] *Donna Curling, et al.* v. *Brad Raffesnperger,* U.S. District Court for the Northern District of Georgia, no. 1:2017–cv–02989, Doc. 768, filed August 7, 2020; *Curling* v. *Raffensperger,* 493 F.Supp. 3d 1264 (N.D.GA. 2020).

[27] *US election 2016: Trump says election 'rigged at polling places',* BBC NEWS (Oct. 17, 2016), *https://www.bbc.com/news/election-us-2016-37673797.*

[28] Bethany Albertson, *Allegations of Fraud Weakened Voter Confidence in the 2016 Election,* THE WASH. POST (Oct. 8, 2020), Allegations of fraud weakened voter confidence in the 2016 election. That could happen again.

[29] Nicolas Berlinski et al., *The Effects of Unsubstantiated Claims of Voter Fraud on Confidence in Elections,* J. OF EXPERIMENTAL POL. SCI. (2021) 1–1, The Effects of Unsubstantiated Claims of Voter Fraud on Confidence in Elections, (cambridge.org); David A. Graham, *The Damage of Trump's Voter Fraud Allegations Can't Be Undone, THE ATLANTIC,* Jun. 19, 2020, Study: Trump's Voter-Fraud Allegations Do Lasting Damage.

[30] David A. Graham, *The Damage of Trump's Voter Fraud Allegations Can't Be Undone,* THE ATLANTIC (June 19, 2020), Study: Trump's Voter-Fraud Allegations Do Lasting Damage.

as a "Full Democracy" by the Democracy Index. Less than two decades later, much has changed. In 2021, the United States was ranked as a "Flawed Democracy," driven by growing efforts at the State and local levels to suppress voting and to subvert legitimate election results. As the Democracy Index's authors explained, "public trust in the democratic process was dealt a blow by the refusal of Donald Trump and many of his supporters to accept the election result" in the 2020 elections.[31] Just this month, an NPR/Ipsos poll found that two-thirds of all Republican respondents subscribe to the "Big Lie" that the election was stolen from former President Trump because of rampant fraud, with fewer than half saying they are willing to accept the results of the 2020 election.[32]

D. The Fabricated Loss of Voter Confidence Is Used To Support the Erection of Obstacles To Voting

Worse still, misguided public sentiment of lost confidence in our election system is then used by lawmakers as justification to impose changes in election practices. Last spring, the *New York Times* studied what they called a "feedback loop" in which falsehoods shape voter attitudes and lawmakers "cite those attitudes as the basis for major changes." The paper counted 33 States where legislators said low public confidence in election integrity was the justification for bills to restrict voting. The report noted an instance where a State legislator asserted such justifications yet was unable to point to evidence supporting the claims about flawed elections, but still claimed restrictive laws were needed because the public believed there were problems. The *Times* noted that misgivings about election integrity are not new, but the scale of the current effort involves many more bills and far reaching restrictions, and the depressed confidence has resulted from an organized disinformation campaign.[33]

In 2021, 19 States enacted 34 laws making it harder to vote, especially for people of color and lower-income people.[34] As the Brennan Center for Justice reported in its most recent summary of pending voting legislation:

These numbers are extraordinary: State legislatures enacted far more restrictive voting laws in 2021 than in any year since the Brennan Center began tracking voting legislation in 2011. More than a third of all restrictive voting laws enacted since then were passed this year. And in a new trend this year, legislators introduced bills to allow partisan actors to interfere with election processes or even reject election results entirely.[35]

Again, Georgia and Texas are illustrative.[36] In Georgia, State legislators responded to the record-shattering turnout of 2020 by passing omnibus legislation, known as SB 202, that restricts the right to vote at nearly every step of the process and disproportionately affects voters of color. Among its provisions, the law requires voter identification in order to request an absentee ballot and vote absentee; severely limits access to absentee ballot drop boxes; and significantly shortens the period in which voters can apply for and cast absentee ballots.[37] These restrictions were adopted right after the November 2020 election where voters of color used ab-

---

[31] *Global Democracy Has a Very Bad Year,* THE ECONOMIST (Feb. 2, 2021), *https://www.economist.com/graphic-detail/2021/02/02/global-democracy-has-a-very-bad-year.*

[32] Joel Rose & Liz Baker, *Six in 10 Americans say U.S. democracy is in crisis as the "Big Lie" takes root,* NPR (Jan. 3. 2022), *https://www.npr.org/2022/01/03/1069764164/american-democracy-poll-jan-6.*

[33] Maggie Astor, *'A Perpetual Motion Machine': How Disinformation Drives Voting Laws,* N.Y TIMES (May 13, 2021), Here's How Disinformation Drives Voting Laws; Isaac Stanley-Becker, *Disinformation Campaign Stokes Fears About Mail Voting,* THE WASH. POST (Aug. 20, 2020), *https://www.washingtonpost.com/politics/disinformation-campaign-stokes-fears-about-mail-voting-using-lebron-james-image-and-boosted-by-trump-aligned-group/2020/08/20/fcadf382-e2e2-11ea-8181-606e603bb1c4_story.html;* Rob Kuznia et al., *Stop the Steal's Massive Disinformation Campaign Connected to Roger Stone,* CNN (Nov. 14, 2020), *https://www.cnn.com/2020/11/13/business/stop-the-steal-disinformation-campaign-invs/index.html;* Jane Mayer, *The Big Money Behind the Big Lie,* THE NEW YORKER (Aug. 2, 2021), *https://www.newyorker.com/magazine/2021/08/09/the-big-money-behind-the-big-lie.*

[34] *Voting Laws Roundup: December, 2021,* BRENNAN CTR. FOR JUST. (Jan. 12, 2022), *https://www.brennancenter.org/our-work/research-reports/voting-laws-roundup-december-2021.*

[35] Id.

[36] See *Georgia State Conference of NAACP* v. *Raffensperger,* N.D. GA. No. 1:21–cv–1259–JPB, filed March 28, 2021; amended May 28, 2021; *Texas State Conference of NAACP* v. *Greg Abbott, et al.* District Court, Harris County, 189th Judicial District, Case no. 2021–57207, filed September 7, 2021. (The Lawyers' Committee is, as are other civil rights organizations, challenging the laws passed by Georgia and Texas described in this testimony.)

[37] SB 202/AP, Section 25, 26 28. *https://www.legis.ga.gov/api/legislation/document/20212022/201498.*

sentee ballots to an unprecedented degree, and in the cases of Black (29.4 percent) and Asian (40.3 percent) voters, at higher rates than White (25.3 percent) voters.[38]

The high turn-out, particularly by voters of color, is evidently part of what prompted the new laws. After the results of the Georgia senate races in early 2021, a Gwinnett County elections official in suburban Atlanta—a county in which people of color have been a growing proportion of the electorate—argued for voter restrictions saying, "They don't have to change all of them, but they have got to change the major parts of them so we at least have a shot at winning."[39] It is no surprise, then, that SB 202 also prohibits the providing of food and drink to voters waiting in line to vote,[40] when it is well-known that in Georgia, voters of color wait to vote for considerably longer periods of time than do White voters.[41]

Despite the actual motivation for Georgia's new law, throughout the debate on SB 202, its supporters attempted to justify the bill using language similar to that used by former President Trump and his allies concerning non-existent election irregularities in the 2020 Georgia Presidential vote. Within days of the election, Representative Barry Fleming, Chair of Georgia's House Special Committee on Election Integrity, publicly likened absentee ballots to the "shady part of town down near the docks" where the "chance of being shanghaied" is significant, and concluded "Expect the Georgia Legislature to address that in our next session in January."[42] Among other things, the preamble to SB 202 indicates that the overhaul of Georgia's election procedures was necessary due to a significant lack of confidence in Georgia election systems, with many electors concerned about allegations of rampant voter suppression and many electors concerned about allegations of "rampant voter fraud." The preamble also asserts the law was designed to "address the lack of elector confidence in the election system," reduce the burden on election officials, and streamline the process of conducting elections by promoting uniformity in voting.[43]

Although the preamble pays lip-service to concerns about voter suppression, SB 202 increases, rather than address, those concerns. Others in Georgia were somewhat more candid. Republican Lieutenant Governor, Geoff Duncan, told CNN that the law was the fallout from a 10-week misinformation campaign by the former President and his allies, including by his personal attorney, Rudy Giuliani, who "showed up in a couple of committee rooms and spent hours spreading misinformation and sowing doubt across, you know, hours of testimony."[44]

Texas passed a law, SB 1, which, among other things, empowers partisan poll watchers with virtually unfettered access in polling places, while at the same time tying the hands of election officials to stop the poll watchers from engaging in intimidating conduct. Texas has a well-documented history of voter intimidation by poll watchers that has disproportionately affected voters of color. The courts have acknowledged this pattern before. In 2014, a Federal district court described this very issue: "Minorities continue to have to overcome fear and intimidation when they vote. . . . [T]here are still Anglos at the polls who demand that minority voters identify themselves, telling them that if they have ever gone to jail, they will go to prison if they vote. Additionally, there are poll watchers who dress in law enforcement-style clothing for an intimidating effect to which voters of color are often the target."[45]

When first introduced in early March 2021, one of the predecessor bills that would become SB 1 stated that its purpose was "to exercise the legislature's Constitutional authority under Section 4, Article VI, Texas Constitution, to make all laws nec-

---

[38] *Georgia State Conference of the NAACP* v. *Raffensperger,* First Amended Complaint, at 47.

[39] Michael Wines, *After Record Turnout, Republicans are Trying to Make it Harder to Vote,* N.Y. TIMES (Mar. 26, 2021), *https://www.nytimes.com/2021/01/30/us/republicans-voting-georgia-arizona.html.*

[40] SB 202/AP, Section 33, *https://www.legis.ga.gov/api/legislation/document/20212022/201498.*

[41] Stephen Fowler, *Why Do Nonwhite Georgia Voters Have To Wait In Line For Hours? Too Few Polling Places,* GA. PUB. BROADCASTING (Oct. 17, 2020), *https://www.npr.org/2020/10/17/924527679/why-do-nonwhite-georgia-voters-have-to-wait-in-line-for-hours-too-few-polling-pl.*

[42] Barry Fleming, *Republican Party wins on Election Day, and future is bright,* THE AUGUSTA CHRONICLE (Nov. 15, 2020), *https://www.augustachronicle.com/story/opinion/columns/guest/2020/11/15/guest-column-republican-party-wins-on-election-day-and-future-is-bright/43155971/.*

[43] SB 202/AP, Section 2, lines 68–148, *https://www.legis.ga.gov/api/legislation/document/20212022/201498.*

[44] See Sara Murray and Jason Morris, *Georgia's GOP lieutenant Governor says Giuliani's false fraud claims helped lead to restrictive voting law,* CNN (Apr. 8, 2021), *https://www.cnn.com/2021/04/07/politics/geoff-duncan-voter-fraud-cnntv/index.html.*

[45] *Veasey* v. *Perry,* 71 F. Supp. 3d 627, 636–37 (S.D. Tex. 2014), aff'd and reversed on other grounds, *Veasey* v. *Abbott,* 830 F.3d 216 (5th Cir. 2016) (en banc).

essary to detect and punish fraud and preserve the purity of the ballot box." Over the course of committee hearings and floor debate on the bill, its sponsor used this "purity of the ballot box" language to defend the Bill. In its final form, the bill still referenced Section 4, Article VI of the Texas Constitution, stating that its purpose was to "make all laws necessary to detect and punish fraud." The final bill included in its first pages a series of "findings," which stated that "fraud in elections threatens the stability of a Constitutional democracy," "reforms are needed to the election laws of this State to ensure that fraud does not undermine the public confidence in the election process," and reforms to the election laws "are enacted solely to prevent fraud in the electoral process and ensure that all legally cast ballots are counted."[46]

Harris County, a Texas county with a large number of Black and Latinx voters was the county that made the greatest use of drop boxes in the 2020 election, and was clearly the target of SB 1's prohibition of drop boxes.[47] But there was no evidence of even minor voting irregularities in the 2020 election in Harris Country or anywhere else in Texas.[48] The Harris County Election Security Task Force issued a final report on the 2020 election, which concluded: "In this election there were nearly 1.7 million votes cast in Harris County. Despite the record turnout, the task force received approximately 20 allegations of wrongdoing that needed to be elevated to the level of a formal investigation. Despite claims, our thorough investigations found no proof of any election tampering, ballot harvesting, voter suppression, intimidation or any other type of foul play that might have impacted the legitimate cast or count of a ballot."[49] The Texas Attorney General's office spent 22,000 staff hours in 2020 investigating voter fraud—more than double the hours spent prosecuting voter fraud cases in 2018.[50] These efforts resulted in 16 minor findings where voters had listed the wrong address on their voter registration card, most of which dated back to the 2018 election. None of these cases resulted in jail time.[51]

It is difficult to overstate the nature of the new bills and laws proliferating in the States. Not only do these laws make it more difficult for voters to vote—whether early, by mail, or in-person—but even more ominously, the new wave of bills and proposals is part of a more comprehensive attack on elections, aimed at facilitating the overriding of the actual votes of the electorate.[52] A group of scholars observed that an effort is under way to change State election rules to "entrench minority rule." They concluded, "This is no ordinary moment in the course of our democracy. It is a moment of great peril and risk."[53] Against the backdrop of January 6, 2021, these statements are not hyperbolic.

IV. CONCLUSION

All this is not to say that changes in election laws are not necessary or that Congress should be complacent about the security of election infrastructure. Far from it. The attack on voting rights is a key to the larger crisis of American democracy. The attack threatens to transform elections into an instrument for a faction seeking to monopolize power and exclude others, rather than a means for expressing "the consent of the governed" as a basis for building consensus to promote the good for everyone. As the letter from the scholars observed, "Defenders of democracy in America still have a slim window of opportunity to act. But time is ticking away,

---

[46] Tex. Elec. Code Section 1.0015 Legislative Intent; Section 1.02 Purpose; Section 1.02, Findings, Senate Bill 1, 87th Tex. Legis., signed into law Sept. 9, 2021 (effective Dec. 2, 2021).

[47] Jen Kirby, *The Battle Over a Texas Order Limiting Ballot Drop-off Locations, Explained,* VOX (Oct. 13, 2020), *https://www.vox.com/2020/10/10/21506522/texas-drop-off-ballot-locations-abbott-harris-county.*

[48] Patrick Svitek, *Harris County Elections Were Fair and Secure, Task Force Finds,* THE TEX. TRIBUNE (Dec. 18, 2020), *https://www.texastribune.org/2020/12/18/harris-county-elections-secure/.*

[49] Id.

[50] Daily Kos Staff, *Texas Spent Another 22,000 Hours Hunting for "Election Fraud" and Didn't Find a Damn Thing,* THE DAILY KOS (June 2, 2021) *https://www.dailykos.com/stories/2021/6/2/2033306/-Texas-spent-another-22-000-hours-hunting-for-election-fraud-and-didn-t-find-a-damn-thing.*

[51] Taylor Goldstein & Austin Bureau, *Ken Paxton's Beefed-Up 2020 Voter Fraud Closed 16 Minor Cases All in Harris County,* HOUS. CHRONICLE (Dec. 21, 2020), *https://www.houstonchronicle.com/politics/texas/article/Ken-Paxton-s-beefed-up-2020-voter-fraudunit-15820210.php.*

[52] Will Wilder et al., *The Election Sabotage Scheme and How Congress Can Stop It,* BRENNAN CTR. FOR JUST. (Nov. 8, 2021), 2021__11__ElectionSabotage(1).pdf.

[53] 53 Statement in Support of the Freedom to Vote Act, Nov. 2021, Democracy letter__November 2021__DocumentCloud.

and midnight is approaching."[54] Congress must reassert its historic role to support free and fair elections and preserve democracy in a moment of peril.

First, Congress must pass the John Lewis Voting Rights Advancement Act (JLVRAA) to restore the strength of the VRA to prevent racial discrimination.

Second, Congress must enact the Freedom to Vote Act (FTVA) to establish uniform minimum standards across the States for early voting, same day registration, voting by mail, fair redistricting, and other essential elements of elections.

The JLVRAA responds to the Supreme Court decisions weakening the VRA, updating the preclearance formula to cover States and localities with a recent record of discrimination, and clarifying the grounds they can use to justify their election laws when challenged. Further, the standards established by the FTVA are common-sense rules prevalent in many States, where there was often bipartisan support.

As Congress proceeds, however, it is important to separate frivolous and fanciful fabrications—intended to inflame passions, shake voter confidence, justify voter suppression laws, and ultimately and perhaps critically injure our democracy—from evidence-based concerns addressed not only to election security, but also to ensuring that voting is easier and more accessible for all Americans.

Chairwoman CLARKE. I thank you for your testimony, Mr. Rosenberg. Finally, I recognize Mr. Masterson to summarize his statement for 5 minutes.

STATEMENT OF MATTHEW MASTERSON, PRIVATE CITIZEN, FORMER SENIOR CYBERSECURITY ADVISOR, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, DEPARTMENT OF HOMELAND SECURITY

Mr. MASTERSON. Thank you, Chairwoman, and thank you, Ranking Member Garbarino and Members of the committee, for the opportunity to testify today. I will skip the introduction as I appreciate the Chairwoman and Ranking Member providing my background I led the work in election security at CISA.

The 2020 election placed election officials at the center of National attention in a way that we haven't seen for decades, if ever. A record turnout and a smooth Election Day validated election officials' incredible work. Yet despite their heroic work, election officials are facing threats against themselves and their systems, their workers, and even their families. This environment is not sustainable and additional support must be provided to these election officials to ensure their safety and the security of our elections.

Recently, myself and a group of students at Stanford published a report on the most pervasive threats facing election officials and the steps we can take to mitigate those. Those threats included physical threats against election officials, the undermining of confidence in election results through a now well-defined playbook available to both foreign and domestic actors, and inconsistent funding and a lack of governance structures around elections' information technology.

There are mitigations to these threats that can empower election officials, further secure our systems, and offer voters the types of evidence needed to reject this mis- and disinformation. These mitigations fall into 3 broad categories: Funding, election officials security, and systems security and resilience.

First, we must fund elections consistently at the State, local, and Federal level. Regular and consistent investment in our elections is needed. A shared funding structure should be implemented in

[54] 54 Id.

which all levels of government pay for their portion of each election.

Second, we must ensure the physical security of election officials, offices, and staff across the country. The recent creation of the DOJ Election Threats Task Force is an important step, but much more must be done. First, the DOJ Election Threats Task Force should provide data after each Federal election regarding the scope and scale of threats against election officials and the workers. Second, in order to ensure comprehensive data is collected, analyzed, and shared local and State law enforcement should be required to share activity directed against election officials and workers with Federal law enforcement in their State. Third, penalties must be increased against those who threaten election officials, workers, or their families. Congress and State legislatures should pass laws offering harsher penalties for threats or acts of violence against election officials or workers. Finally, CISA should offer training and guidance on physical security and doxing prevention measures that election officials can take, utilizing the protective security advisors, like those in Region 2 that the Ranking Member mentioned, in order to train election officials.

Finally, we must continue to improve the cyber resilience of American elections. This starts by encouraging States to implement precertification audits of paper ballots. Second, CISA and the EI–ISAC should provide more proactive, scalable service to election officials, like Crossfeed as was mentioned by the Ranking Member, a service that was provided in 2020. This should include expanded use of Crossfeed in both scope and scale, remote incident response services, and increased endpoint protection and email protections for mid-to-small counties who struggle to protect their systems.

Third, we must better define the Federal roles and responsibilities in elections. Congress should further clarify the roles of CISA and the EAC, making CISA the technical lead for election security while empowering the EAC to better focus on its other election administration missions. Creating well-defined responsibilities for CISA and the EAC will allow both agencies to fully achieve their core missions, eliminating the on-going Federal infighting regarding roles and responsibilities, and creating clear lines of communications for election officials on these issues. This should include moving the Federal voting system testing and certification program to CISA.

Third, CISA and EI–ISAC in partnership with election officials should establish core cybersecurity baselines for election offices. These baselines should include, at a minimum, required multifactor authentication for all critical systems, a move of all election websites to .gov, increased access controls, more efficient and effective patch management, and proper network segmentation of election networks away from State and local county networks. In establishing these baselines, CISA should leverage its on-going support to election offices to inform the scope and scale of implementation of these baselines, as well as additional steps election offices can be taking to secure their infrastructures.

Our elections are imperfect. They are massive, messy, underfunded, and under-resourced. But they are accurate, secure, accessible, and fair because of the tireless work of State and local elec-

tion officials. The only response to the on-going threats against our democracy is a sustained investment in those working hard to protect it.

I appreciate the time and I look forward to your questions.

[The prepared statement of Mr. Masterson follows:]

PREPARED STATEMENT OF MATTHEW MASTERSON

JANUARY 20, 2022

Chairwoman Clarke, Ranking Member Garbarino, and Members of the committee, the 2020 U.S. election was unprecedented in American history. While many have detailed what went wrong (or right), reports have largely overlooked the group most impacted by these changes: State and local election officials. Election officials anticipated problems, quietly pivoted with each changing health measure and court case, and faced many of the worst repercussions of viral and inflammatory misinformation. In the end the 2020 election was secure and accurate because of their hard work and commitment to our democracy.

Trust in American elections is under attack from abroad and at home. The Federal Government's support framework, while improved, remains challenged to effectively ameliorate the issues election officials face. The threats are real and evolving. Immediate support and investment must be provided to these officials in advance of the upcoming mid-term elections and the 2024 Presidential election.

THREATS TO ELECTION PROCESSES [1]

1. Election officials' capacity to do their jobs is degraded by physical threats and broad distrust fomented by bad-faith actors.—These threats undermine officials' ability to conduct critical community outreach, and could contribute to brain-drain at a time when competence at the local level is needed most.

2. The playbook for undermining confidence in election results is well-defined and available for foreign and domestic influence agents.—The 2020 election prominently featured attempted election interference from foreign and domestic actors. Influence agents are emboldened by 2020, while defenders of election integrity are under-resourced and uncoordinated, leaving them vulnerable to repeated tactics.

3. Inconsistent funding and lack of governance structures around elections IT continue to perpetuate vulnerabilities.—Despite marked progress since 2016, emerging threats such as ransomware continue to expose critical election systems to crippling attacks. In defending election systems, under-resourced local governments face off daily against well-funded nation-state adversaries, a disparity that continually exposes election systems to attack.

RECOMMENDATIONS

In light of the aforementioned threats, and others yet to come, below is a set of concrete and actionable recommendations to shore up election security and ensure election confidence. Each of these recommendations will require coordination by relevant stakeholders at the local, State, and Federal level.

Fund elections consistently at the State, local, and Federal level

Every year, State and local election officials across the country struggle to obtain the funding needed to run elections. State and local governments often push aside pleas in favor of issues perceived as more immediate, passing over electoral needs that are commonly viewed as seasonal despite elections that are run several times a year in most jurisdictions. Almost every election official is commonly asked "What do you do the other 364 days a year?" when discussing the operational challenges of their work.

Securing election infrastructure is a matter of National security. This is precisely why the Department of Homeland Security designated election systems as critical infrastructure in 2017. Elections should be funded commensurate with their status as critical infrastructure, with all levels of government ensuring regular and consistent funding. A shared funding structure should be implemented in which all levels of government pay for their portion of each election. This practice is done locally in several States and is sometimes referred to as "charge backs" or the "ballot real

[1] This testimony is based in large part on a Stanford Internet Observatory research paper: "How to Secure American Elections When the Losers Won't Accept They Lost" by Matt Masterson, Jennifer Depew, Katie Jonsson, Shelby Perkins, Alex Zaheer.

estate" model. The idea is that each jurisdiction that appears on a ballot in any given election is charged for its portion of that election. For instance, if an election has a Congressional race, State house race, mayor's race, and county commissioner race, then the Federal Government would pay for the cost of the House race, State government for the cost of the State house race, city government for the mayor's race and the county for the cost of the commissioner's race. This would ensure consistent and regular funding of elections, with each level of government paying its share of the cost.

Congress should establish an elections fund, administered by the U.S. Election Assistance Commission (EAC), that State election officials can draw down from based on the expense to run Federal elections in their State. States should be required to pass the majority of the money down to their local officials to cover the additional costs of running Federal elections. This funding structure will incentivize deliberative, planned investment that allows for risk-based decision making and funding for human capital, systems acquisition, and processes to ensure sustainability of those systems over time.

Ensure the physical security of election officials, offices, and staff across the country

Many State and local election officials faced threats of violence due to mis- and disinformation about the 2020 election. In many cases, officials who reported these threats received little to no support from local, State, or Federal law enforcement officials. Many of the threats were deemed not serious or imminent enough to necessitate action.

More must be done to protect the health and safety of election officials and election workers, including private-sector employees who support elections. The recent creation of an Election Threats Task Force at the Department of Justice (DOJ) is an important and encouraging first step. The following steps to further protect election officials:

1. Publication and use of threat data.—The DOJ Election Threats Task Force should provide data after each Federal election regarding the scope and scale of threats against election officials and workers. This report should include the number of complaints, number of credible threats, number of acts of violence and number of prosecutions for those threatening election officials or workers. This data would support efforts at the State and local level to prioritize funding for physical security, shore up gaps in security and better diagnose on-going problems. In addition, based on this data, the DOJ task force, in coordination with CISA, should release guidance on best practices for election officials, counties, States, and the Federal Government to better protect those who run elections.

2. Increased information sharing regarding threats.—From our interviews with election officials, it became clear that Federal, State, and local law enforcement are not sufficiently coordinated regarding the scope, scale, and regularity of threats against election officials. This is particularly concerning because existing structures are in place, including State fusion centers, to facilitate this information sharing. In order to ensure comprehensive data is collected, analyzed, and shared, local and State law enforcement should be required to share activity directed against election officials and workers with Federal law enforcement in their State. In return, Federal law enforcement should regularly report back to State and local officials regarding the activity in their jurisdiction with full transparency regarding any actions taken, including if investigations have been initiated.

3. Penalties.—Congress and State legislatures should pass laws offering harsher penalties for threats or acts of violence against election officials. Following the 2020 election, there have been few consequences for those who threatened election officials. Any potential violence against election officials or workers should be treated as a threatened attack on the process and democracy itself, and should result in criminal liability.

4. Privacy.—Many threats against election officials and staff directly target their homes and families. More must be done to protect their private information from would-be malicious agents. Many States have passed laws that protect the identity of certain subsets of registered voters. These categories typically include law enforcement officers, judges, and domestic abuse victims. Election officials should be included in this category to ensure that their personal information is not readily available publicly.

5. Prioritizing protection of election officials and workers.—State and local law enforcement should treat threats against election officials as credible. This may mean increasing patrols around offices and residences, as well as further investigation into additional threats. Because State and local law enforcement often lack sufficient funding, State legislatures and county governments should provide additional

funding to support the protection of election offices and workers, especially during and after election periods.

6. Physical security and doxxing training.—CISA should offer training and guidance on physical security and doxxing prevention measures. CISA has protective security advisors (PSA) located across all 50 States to advise on physical security matters. These PSAs have done a great job working with local election officials to evaluate the physical security posture of local offices and storage facilities. PSAs should offer additional support and training to help election officials protect themselves and their staff from doxxing and physical harm away from the office.

Encourage States to implement paper-based pre-certification audits

No single improvement to the security of elections was more important in 2020 than the wide-spread use of auditable paper ballots. Approximately 95 percent of votes cast in the 2020 election were on an auditable paper ballot, up from just over 85 percent in 2016. In Georgia, election officials could hand-audit ballots to show the accuracy of the election results. In Maricopa County, Arizona, the election officials conducted the State-required public hand audit by bipartisan recount boards. The results of this hand audit affirmed the results of the election in the county.

States should prioritize implementation of paper ballot audits that are completed before vote counts are certified. These audits should offer a transparent, bipartisan, and repeatable process by which the results of the election as tabulated by the voting systems can be evaluated through the review of the paper ballots.

In pursuing better, more efficient pre-certification audits, States should also continue to pursue evidence-based elections. This means implementing systems, processes, and procedures that maintain transparent records of the integrity of the election. An audit is only as good as the integrity of the artifacts to be audited. For elections, this means that chain of custody of the ballots and proper ballot manifests are imperative to the trustworthiness of the audit. As part of the implementation of these post-election audits, States should support local election offices in implementing consistently documented chain of custody and ballot tracking procedures across the State.

Reform the Federal voting system certification process

The process for voting system testing and certification must be reformed. Election officials have been forced into maintaining outdated and unsupported systems for longer than their expected lifespan in part because the EAC process has not evolved to support items like component certification, regular patching of systems and further deployment of commercial off-the-shelf technology. While EAC commissioners have committed to the pursuit of these items as part of the roll-out of the Voluntary Voting System Guidelines (VVSG) 2.0, the passage of VVSG 2.0 as the same monolithic standard as the prior VVSG makes it unlikely that the process can be reformed enough to be responsive to the needs of election officials.

Congress should further clarify the roles of EAC and CISA in elections, making CISA the technical lead while allowing the EAC to better focus on its other election administration missions. Both EAC and CISA have limited resources and capabilities, so further clarification of roles and responsibilities would allow each agency to best use its time and money in support of the election community. CISA is the more technically capable organization and should be formally designated as the lead Federal agency for the physical and cybersecurity support of election systems and officials. This should include moving the Federal Voting System Testing and Certification Program to CISA. The National Institute of Standards and Technology (NIST) should remain in its HAVA-created role as technical consultant on the development of the VVSG.

The EAC should be empowered to focus on all other aspects of the election process beyond cyber and physical security issues, allowing it to build out its clearinghouse function, advancing data collection and research efforts, and continuing to disperse election grants provided by Congress. Creating well-defined responsibilities for CISA and EAC will allow both agencies to fully achieve their core missions, eliminating the on-going Federal infighting regarding roles and responsibilities and creating clear lines of communication for election officials on these issues.

In addition, regardless of who runs the program, the Federal testing and certification process should be reformed to address the marketplace challenges it is creating:

1. Already certified voting systems running unsupported operating systems should be decertified.—Because these systems are running unsupported operating systems, they are unable to be patched to remediate known vulnerabilities. Most of these systems cannot simply be updated because they lack the memory or processing power to run updated operating systems. Many

election officials running these systems have expressed the need to replace them, but have not received the necessary funding to do so. Voting system vendors and election officials should be notified of pending decertification and should be given enough time to upgrade or replace their systems.

2. VVSG 2.0 should be implemented rapidly.—This would mean that all new systems submitted to the certification program must be VVSG 2.0-compliant to receive certification by a date established by the EAC in the near future. The certification program should avoid using metrics like accreditation of the voting system test laboratories to conduct VVSG 2.0 testing or certification of the first voting system to VVSG 2.0 as metrics for sunsetting VVSG 1.0 and 1.1. In setting a date, the certification program should publish a definition of what constitutes a new voting system and make clear that this definition will be enforced. In the past, vendors have avoided certification to the newest standards, such as VVSG 1.1, by modifying already certified systems, allowing them to be tested to the older standard in perpetuity.

3. The certification program must incentivize patching of voting systems.—Currently, the certification process disincentivizes regular patching of systems by requiring testing (sometimes extensive) of most software updates. This causes voting system vendors to hold off on pursuing modifications to systems until they reach a critical mass of changes that justify the financial and time costs associated with certification. Instead, the certification program should revise its policies to allow vendors to attest to their own testing of critical patches on already certified systems. In allowing for vendor attestation, the certification program should require the voting system test laboratories to review and approve vendor testing documents prior to approval of the patch. This process should be expedited to allow for timely deployment of patched systems to the field, recognizing that the majority of voting systems cannot be remotely patched. This process would be separate from the existing de minimis change process, which requires no additional testing by the vendor or test lab to receive approval.

Provide election offices more scalable and proactive services through CISA and EI–ISAC

Given the vast and decentralized nature of election administration in the United States, the challenge for CISA and the EI–ISAC is immense. How do you ensure that information, support, and services reach the smallest town in Wisconsin or the most remote county in Montana? Even if you reach those places, how do you make the information and services relevant and usable for the election official in Jackson County, Ohio? CISA and the EI–ISAC have made incredible progress on this challenge since the 2016 election. All 50 States, Washington, DC, and the 4 territories joined the EI–ISAC; intrusion detection sensors were deployed on election infrastructure across all 50 States; thousands of State and local offices participated in tabletop exercises; hundreds of cyber hygiene scans were conducted; and virtually every State received a penetration test.

Even with the success of these offerings, the scalability of the services remains a challenge. Due to resource constraints, CISA can only perform a finite amount of on-site vulnerability assessments of all critical infrastructure, let alone elections. In addition, many election offices do not have the necessary IT resources to benefit from some of the more in-depth services. Over the last 4 years, CISA has learned the intricacies of the election sector and the systems that support it. It has worked to prioritize the services that are most useful, and it has developed new and scalable services, such as remote penetration testing, to better serve the community.

In 2020, CISA recognized that it needed to be more proactive in its work with election officials. In collaboration with the Defense Digital Service, the agency developed and released a tool called Crossfeed, which is used to gather information about vulnerabilities on public-facing systems supporting critical infrastructure. Crossfeed proactively collects data through a variety of open-source tools, publicly-available resources and data feeds, and can operate in a "passive" mode where it relies on unintrusive data-gathering methods.

Moving forward, CISA and the EI–ISAC should learn from the success of Crossfeed to identify and provide additional proactive, scalable services to local election offices. Both entities have built a level of trust with election officials that means they can afford to be more aggressive in the types of support provided. For example:

1. CISA should expand the Crossfeed program.—Recently CISA announced the continuation of Crossfeed. This is an important first step. The agency should expand the use of the program to include offering all 50 States, the District of Columbia, and the territories active participation in the program with the goal of proactive monitoring of publicly-available aspects of State and local offices' infrastructure. This should also include the use of Crossfeed on other election-

specific technology, such as proactively searching for voting systems that may be inadvertently connected to the internet. Further, CISA should offer the service to election vendors, campaigns, and other election-related entities.

2. CISA should offer remote hunt and incident response to election offices.—Like on-site vulnerability assessments, CISA hunt and incident response services have traditionally involved on-site deployment of responders to an office. This makes both services extremely labor-intensive and difficult to scale. CISA has piloted some remote incident response capabilities in the past, and it is time to expand this effort along with proactive network hunt capability.

3. EI–ISAC should expand its endpoint protection program.—Throughout 2020, EI–ISAC worked with some State and local offices to pilot endpoint protection for their offices. This pilot proved to be useful for both the election officials and EI–ISAC as it worked to gain greater insight into the scope of activity targeting election infrastructure. This program should be expanded to more jurisdictions, with a focus on medium-to-small localities that lack the same or similar capabilities and would benefit most from these services.

4. EI–ISAC should offer cloud-based email as a service to local election offices.—Email security is one of the largest risk areas for local election offices. Many continue to run outdated and unpatched email servers with little ability to upgrade and maintain them. EI–ISAC should partner with Microsoft, Google, or other large cloud-based email providers to explore implementation of email as a service for local election offices and county governments. For counties that are unable or unwilling to implement a State-based solution, the EI–ISAC could be a viable solution from a trusted partner.

5. EI–ISAC should provide a managed solution for multi-factor authentication (MFA).—Many election offices continue to struggle to implement MFA across their systems. While there are a lot of MFA solutions available in the marketplace, many election offices are unable to implement MFA because of outdated legacy systems and lack of vendor support. EI–ISAC should work with State and local offices to understand the full scope of the challenge and coordinate with a commercial provider to offer a managed solution for local offices to implement MFA on general office systems. In providing this service, EI–ISAC should offer technical support and resources for MFA implementation in existing election legacy systems. In addition, EI–ISAC should partner with common election system vendors to make it easier to implement MFA, as well as encourage these vendors to implement MFA themselves. Election-specific systems may be harder to include in this effort because of strict requirements around certification and implementation.

Mandate reporting of election cyber incidents to CISA and the FBI

Improved and increased information sharing regarding election cyber incidents was an incredibly important development for the protection of the 2020 election. Federal, State, and local officials worked together to understand possible incidents and support response efforts in unprecedented ways. Moving from distrust seeded by the fallout of the 2016 election to this level of partnership is a tribute to the professionalism and commitment of State and local officials.

Building on this progress, Congress should require State and local election offices and private-sector election providers to report cyber incidents to CISA and the FBI. This is a necessary step for two main reasons. First, CISA and the FBI have no ability to mandate this type of reporting themselves. While the vast majority of possible incidents in 2018 and 2020 were shared with the Federal Government, some were not shared with either the Federal Government or State officials. Time is of the essence during any cyber incident, but even more so with elections as officials work against a hard deadline and with limited resources. Required reporting will ensure timely and coordinated response from all levels. Second, given the sophisticated and persistent nature of the threats against elections, ensuring the Federal Government has a full picture of the activity out in the field is critical to providing a whole-of-Government response to officials. The full capability of the Federal Government can only be brought to bear to protect election systems when the agencies charged with support of their defense have full visibility into the tactics, techniques, and indicators of compromise employed by adversaries.

Establish minimum cybersecurity baselines for State and local election offices and election vendors

In July 2021, the White House issued a "Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems." The memo pushes Federal agencies to work more collaboratively with private-sector companies that own and operate critical infrastructure systems to advance basic cyber practices. The memo requires

agencies and the private sector to jointly establish voluntary guidance for the cybersecurity of critical infrastructure systems.

CISA, the Government Coordinating Council (GCC) and the Sector Coordinating Council (SCC) should work together to publish a set of minimum cybersecurity practices that all election offices and companies should adopt. These practices should recognize that the majority of U.S. election jurisdictions are mid-sized to small counties, cities, and townships that lack sufficient funding or IT support. We recommend starting with the NIST cybersecurity framework and adding or emphasizing the following:

1. Create and Maintain an Inventory of Assets.—For many election offices, items like patch management and incident response are hindered by a lack of understanding of what systems and software the office owns and operates. Election offices should create and maintain an enterprise-wide inventory list with up-to-date information on system type and version.

2. Require Multi-factor Authentication.—All critical systems, including business systems like email and voter registration access portals, should require MFA for all users.

3. Ensure Network Segmentation.—All local election networks should be properly segmented from each other and other county networks. Proper segmentation greatly reduces the ability for malicious actors to access or impact election networks after compromising another county department or system.

4. Maintain Access Control.—All election-related systems should follow the rule of least privilege. This means that only those that need access to a system should be given access, and only the access they need to accomplish their work. This should be applied to vendors and staff alike.

5. Utilize Patch Management.—Implementing a patch management program reduces the likelihood of an organization having a cybersecurity incident particularly as a result of commodity malware.

6. Move to .gov.—All State and local election websites should be moved to a .gov domain name. This is important for both security and to help combat mis- and disinformation, as .gov domain names are recognized as trusted government websites. CISA is offering .gov domains for free and is scaling up support to help States and localities move their websites over.

Centralize election IT infrastructure at the State level

With the passage of the Help America Vote Act (HAVA) in 2002, many States took on much more responsibility for election administration. HAVA's requirement for the creation of State-wide voter registration databases and requirement for the establishment of a chief State election official gave election leadership to several States that previously had little or no role in the administration of elections. For many of these States, it forced a partnership between the State and localities that administered elections that never existed before. As States worked to implement HAVA, many experienced pushback, and even outright hostility, from localities that previously had sole responsibility for administering elections.

In time, local and State election offices have largely worked through those challenges and established defined roles and responsibilities for the administration of elections, including voter registration databases. Some States took full control, running top-down, State-wide voter registration databases. Others left control largely in the hands of the localities, serving simply as an aggregator of data at the State level, running bottom-up registration databases. Still, others have a hybrid system with a mix of top-down and bottom-up characteristics. Over time, these lines were further blurred with States taking on additional responsibility for military and overseas voters, with many beginning to offer sample ballots, voter look-up tools, and ballot tracking.

The 2016 election permanently changed the threat landscape for elections. Russia, a nation-state adversary, was able to research, remotely target and, in a small number of cases, access election systems. This change in threat level must be met with a change in governance structure at the State and local level. Since HAVA, States have proven themselves capable of supporting elections by handling more responsibility for the administration and corresponding infrastructure of elections. In most cases, compared to local governments, States possess significantly greater budgets, staff, and capabilities to protect from, detect, and recover from cyber attacks against election infrastructure. Recognizing this, we recommend the following steps.

1. Move to top-down voter registration systems.—In many cases, the decentralized nature has served election administration well. It has created flexibility for local election officials to creatively solve challenges unique to their county or township. However, voter registration systems are among the areas of greatest

risk, according to a risk assessment release by CISA in 2020. Bottom-up States in particular have an increased attack surface and more risk to manage.

It is time for States to take on the full responsibility of HAVA and move to top-down voter registration systems. Local election offices should not be asked to bear the responsibility of managing and securing these increasingly complex and important election systems. This move will also free up much-needed resources for local election offices to spend on other areas of election security and administration. A move to top-down voter registration across all States also will create an opportunity for the community to work collaboratively with CISA to create guidelines and new methods for securing and auditing voter registration systems, something that is difficult to do now because of the diversity of systems and infrastructure among county systems.

2. Provide State-managed email accounts.—Many cyber incidents begin through the compromise of a local email account that is used to compromise other systems. A substantial number of localities maintain their own email servers. In many cases, this results in the administration of an email server within the county, sometimes by the local election office itself. In other cases, the local election office is left without any email support and is forced to use its own email account, sometimes resulting in the use of personal email accounts. States should utilize existing infrastructure to offer local election offices their own email accounts through the State, including cloud-based email services that the State is already using for its own email systems. If State-managed email accounts can't be offered, States should offer localities access to Microsoft or Google cloud-based email services. Both of these companies have offered additional protections and default secure configurations to election customers, and would greatly lower local offices' risk profile.

3. Broaden implementation of cyber navigator programs.—Following the 2016 election, State election officials and their IT leads quickly came together to evaluate risk, strategize on mitigations and assess next steps in better defending their infrastructure. As they secured their own systems, State IT leads knew that the greatest risk rested across the machines maintained by counties, townships, and cities that are actually responsible for running elections. Most recognized that State-level investment in local support would be necessary to properly manage the new risk environment. To shore up capability gaps at the local level, Illinois implemented a program dubbed the "Cyber Navigator Program" that provided State-funded IT leads to help localities evaluate risk posture and implement a checklist of steps to improve security and resilience. Several States, including Florida and Minnesota, implemented similar programs. Iowa took a similar approach, partnering with State and county IT leads to help local auditors secure election systems. This included engagement with the Iowa National Guard as well as cross-county support to ensure lesser resourced auditors received services and support. Moving forward, more States should implement similar State-funded programs to ensure that all county election offices have consistent and reliable IT support before and during elections.

Support good-faith security research and vulnerability assessments

Since the passage of HAVA and wide-spread adoption of electronic voting systems, security researchers from academia and industry have focused their attention on the vulnerabilities in those systems. The quality of the relationship between the research community and election community has ebbed and flowed from highly contentious to begrudging respect.

Following the 2020 election, as election officials and industry were besieged with claims of rigging and hacking, security researchers saw their work distorted in pursuit of untoward goals. In an effort to defend both their work and the security of the 2020 election, researchers spoke out with one voice, making clear that "[m]erely citing the existence of technical flaws does not establish that an attack occurred, much less that it altered an election outcome" and calling the claims "technically incoherent." There is an opportunity now for these two groups to find common ground and support each other in improving both the security of election systems and confidence in the process. This can be done in several ways:

Adopt Vulnerability Disclosure Policies (VDP)

A strengthened relationship between election administrators and security researchers should start with States opening to good faith research through further adoption of vulnerability disclosure policies (VDP). These policies provide a safe haven for security researchers to find vulnerabilities in public-facing election systems and report them to the State election office for remediation. The Ohio Secretary of State's office was the first election office to implement VDP, with Iowa fol-

lowing closely behind. Other States have since announced their intention to implement a VDP. In addition, some of the largest voting system providers have announced creation of their own VDP, with four of the largest vendors currently offering VDPs. In 2020, CISA released a "Guide to Vulnerability Reporting For America's Election Administrators" that focuses on empowering election officials to create and implement their own VDP programs. VDPs not only build a bridge between the two communities, but also provide under-resourced election offices access to top-level security assessments at essentially no charge.

Moving forward, all 50 States and election technology providers should implement VDPs for their organizations. The VDPs should follow industry standard practices and include legal safe harbor to authorize testing and protect researchers. States should also consider requiring election system providers to have an existing VDP in order to be eligible to receive contracts. In addition, EI–ISAC should work with its executive board to create and implement a VDP that allows researchers to report vulnerabilities in local election infrastructure to the EI–ISAC, which would then notify the appropriate vendor or office. In serving in this role, EI–ISAC should work with the local election offices to determine the validity and severity of a report, as well as possible mitigation strategies. EI–ISAC should commit to collecting and reporting on the amount and types of vulnerabilities reported, and work with CISA to publish guidance on remediation of the most common vulnerabilities.

Expand open-ended vulnerability assessments

Starting in 2019, CISA began offering election system providers access to Critical Product Evaluations. These are open-ended vulnerability assessments of the submitted system that is part of critical infrastructure. Testers tear apart systems looking for hardware, firmware, and software vulnerabilities, issuing a report when finished of the discovered vulnerabilities and their severity. This type of open-ended vulnerability assessment has been discussed for decades, but has never taken hold in part because the Federal testing and certification process is not properly structured for it.

In the aftermath of the 2016 election, DEF CON, the world's largest hacking conference, created a Voting Village, self-described as "an open forum to identify vulnerabilities within U.S. election infrastructure and to consider mitigations to mitigate these vulnerabilities." The Voting Village has exposed a broader range of security experts to the inner workings of election systems and brought election officials into the room with those experts to understand the mindset of a hacker. The village has also elevated election system security as the National security issue that it is. However, since its inception, the Voting Village has been controversial with some within the election community because of its unwillingness to provide context around the procedural controls that exist in elections. In addition, some organizers of the Voting Village openly mocked election officials, going so far as to describe them as "f—ing luddites."

Bridging the gap between election officials and the security community through open vulnerability assessments is critical to continuously improving the security of elections. Doing so will increase the number of third-party experts available with exposure to election systems, allowing them to credibly affirm and amplify election officials' debunking of false claims made regarding the security of the systems.

Moving forward, the following steps should be taken to increase the exposure of election systems to third-party security research.

1. Expansion by CISA of the Critical Product Evaluation Program.—For many vendors, this is an important introduction to open-ended vulnerability assessments and allows the vendor to understand the level of effort needed to mitigate vulnerabilities found during open-ended testing. CISA had robust participation in the evaluation program throughout 2019 and 2020 with many of the largest voting system companies participating. However, due to interest from other areas of critical infrastructure and limited capacity, CISA could not evaluate every system that was requested to go through the program. CISA should prioritize resourcing to allow any election system provider to submit its system to the program and receive an evaluation prior to the 2024 election cycle. In addition, CISA should continue outreach to private-sector election system providers to increase the diversity of the types of systems submitted, including voter registration providers, election night reporting providers and electronic pollbooks. While these evaluations are useful for vendors themselves, making these evaluations public after sufficient review would significantly improve awareness of potential product security concerns for election officials looking to make acquisitions.

2. Private-sector participation in the DEF CON Voting Village.—The Voting Village has served an important role highlighting the National security importance

of election systems. The Voting Village is an important forum for voting technology companies and election officials to engage with the security research community, but its value is currently limited because of the lack of new systems made available at the conference. Moving forward, the Voting Village should work more collaboratively with industry and election officials to secure relevant election systems for the conference. This will likely mean establishing protocols for the village to include vendor participation and responsible disclosure processes when vulnerabilities are discovered. This is typical across many of the villages at DEF CON, including the Aerospace and Healthcare villages. For their part, election technology providers should recognize the value that DEF CON participants can bring to evaluating systems, particularly for systems in development, and actively participate in the village instead of shunning it as unproductive.

3. Incorporation of vulnerability assessments into the Federal certification process.—Whether vulnerabilities are discovered during CISA's Critical Product Evaluation, at the DEF CON Voting Village, or through other channels, the ability for the Federal certification process to intake those vulnerabilities and work collaboratively to respond to them is critical to deploying mitigations in the field. Currently, the EAC has no formal mechanism to intake reporting from independent third parties regarding voting system vulnerabilities. This leaves the EAC in the dark and unable to respond to discovered vulnerabilities. The certification program must create a process by which it intakes vulnerability reporting for certified systems and works with vendors and election officials to respond. In addition, the certification program must reform its standards development process to nimbly incorporate vulnerability reporting into the feedback loop in order to inform revisions to the VVSG.

4. Eliminate legal barriers to security research.—Too often, especially in the elections space, security researchers are deterred from testing for or disclosing vulnerabilities due to fear of legal action. Specifically, Section 1201 of the Digital Millennium Copyright Act (DMCA) and the Computer Fraud and Abuse Act present legal risk for security researchers. While the U.S. Copyright Office has added security research exemptions via the triennial rule-making process, the exemptions are too narrow and only temporary. Congress should codify strong security research exemptions for the DMCA into law. Further, Congress should explore similar security research exemptions for the Computer Fraud and Abuse Act, contingent on a good-faith, harm-minimizing research approach and researchers making an attempt to disclose any discovered vulnerabilities.

CONCLUSION

While the progress made in the 4 years between Presidential elections was immense, it was only a beginning. Following the 2020 election, much of election official's energy and attention has turned to responding to mis- and disinformation. This is understandable given the scope and volume of mis- and disinformation they faced throughout 2020 and since, but could result in underappreciating the resources or attention necessary to improve the security of their systems. In an environment where the loser of an election may not accept the result no matter the margin of victory, the ability to show the resilience and security of the process is more critical than ever. Continuously improving security measures, alongside better tools to fight mis- and disinformation as it arises, are the keys to building confidence in future elections.

For the foreseeable future, election administrators will be in the spotlight, forced to deal with advanced and persistent cyber threats, as well as physical threats of violence driven by mis- and disinformation targeting our democracy. The spotlight is bright and unrelenting, and more must be done to empower election officials with the tools to deal with it. The alternative is a world in which the hard-won progress of the security and accessibility of our elections is a casualty of a caustic political environment driven by greed and a thirst for power rather than the higher ideals of our democracy.

Chairwoman CLARKE. I thank you and all of today's witnesses for your testimony. I will remind the subcommittee that we will each have 5 minutes to question the panel. As I begin, I now recognize myself for questions.

As I said in my opening, if election security means anything, it means, No. 1, making sure every voter can cast their ballot; and, No. 2, that their ballot will be counted. Mr. Rosenberg, you talked

about how politicians have exploited the perception of low voter confidence as a pretext for laws that make voting harder, but not more secure. What do you see as the real threat to voter confidence and how has it changed since the 2020 election?

Mr. ROSENBERG. Well, thank you for that question, Chairwoman Clarke. The real threat we see is the lies. Because what happens is the lies create lack of voter confidence. Then you have those lawmakers who are intent on suppressing the vote of people of color in order to stay in power, using the surveys that reflect this so-called lack of public confidence in what has been called a feedback loop, that is then used to support, to provide justification, they say, for laws. We have seen it happen in Georgia, in the passage of S.B. 202, in which, among other things, it makes it more difficult to apply for and cast absentee ballots at a time when voters of color were using absentee ballots more than White voters were using in the 2020 election. Even prohibiting the provision of food and water to people who are waiting in line when it is known that in Georgia, for example, Black voters are waiting an average 9 or 10 times longer in line than are White voters. So, it is those kinds of things that we see are the biggest threats.

Chairwoman CLARKE. Well, thank you. Ms. Ramachandran, how has this misguided notion of a rigged or stolen election actually jeopardized the security of the people and systems that run our elections?

Ms. RAMACHANDRAN. Thank you so much for that question, Chairwoman Clarke. This Big Lie that has been spread around the 2020 elections has really endangered our election infrastructure in a number of ways.

One of the primary ways it has endangered our system is that it has encouraged and given a boost to this wide-spread push for these sham partisan reviews. These sham partisan reviews have multiple times resulted in valuable election equipment having to be decertified or decommissioned because in a legitimate election audit, the ballots and the election equipment stay in the custody of the election officials or a certified Federal voting system testing laboratory. They are not handed over unsupervised to partisan outside contractors. Once that happens, then there is a risk that something malicious has been inserted into the equipment or that something has been done to disrupt it, and that is what has led to some of this equipment having to be decommissioned and decertified. So, that is a really huge risk that comes from the Big Lie, the spread of these partisan reviews.

Another risk is that all of this disinformation is leading to attacks on the election officials and election workers who have done such a heroic job in providing us with free and fair elections. Those attacks are causing them to be deterred from doing their jobs, pushed out, resigning. They are part of our election infrastructure. They are the personnel that make the system work.

Then finally, the lie may be leading some small number of election officials and workers to actually be susceptible to entreaties that they provide unauthorized access to election conspiracy theorists. This has happened already a few times in some small instances in the United States. I mentioned the one in Colorado.

There has been some unauthorized access provided in Ohio and Michigan, as well.

Chairwoman CLARKE. Well, thank you. Mr. Stamos, you have suggested the need for clear Federal authorities around mis- and disinformation. I have a bill to do just that, giving CISA clear authorities to build on efforts like the Rumor Control website. What more do you think CISA could be doing on mis- and disinformation?

Mr. STAMOS. Thank you, Chairwoman. I think a key function that we need to have somewhere in the Executive branch is the ability to understand what kind of misinformation/disinformation is currently dominating the discussion on-line. This is not going to be just around elections. Right? We have the same problems around vaccines. If there is a natural disaster, we end up with significant disinformation issues. If we had a plane crash today, a tragedy, there would be conspiracy theories and disinformation being spread. I think that is one of the things that Congress should consider is where should that capability exist?

The capability is really just about understanding what is going on. But I don't think it is realistic for Health and Human Services, the FAA, FEMA, for every part of the Government to have a group that can do the kind of deep social media analytics that is needed in these kinds of situations, and I think CISA is probably the place that you want to at least start.

Chairwoman CLARKE. Thank you very much. My time has elapsed. I now recognize the Ranking Member of the subcommittee, the gentleman from New York, Mr. Garbarino, for his questions at this time.

Mr. GARBARINO. Thank you, Chairwoman. I appreciate all the witnesses' testimony so far.

First, I want to start with Mr. Masterson. You have, as we have talked about with your bio, you have first-hand experience administering elections at the State level. State and local, and as you know, State and local election officials play a tremendous role in facilitating secure elections. On top of this already complex and burdensome responsibility, officials in New York are now faced with the difficult task of allowing non-citizens to vote, thanks to the new mayor, New York City Mayor Eric Adams' decision to grant more than 800,000 non-citizens the right to vote in municipal elections.

The New York State constitution is clear. Its citizens are the ones who have the right to vote. But my question to you is what are your thoughts about allowing non-citizens the right to vote in addition to what are your thoughts about how this is going to affect the election officials and their ability to do their jobs?

Mr. MASTERSON. Yes, thank you, Ranking Member. First of all, it is important to note that for Federal elections non-citizens cannot register or vote in Federal elections, which I think is appropriate. Any time election officials are presented with additional responsibilities that include the use of more databases, more registration, separate registration activity, that adds a layer of complexity to their work that needs to be met both in resourcing and in support. So, any time we talk about changes like this and looking at sort-of the risk analysis that applies, we have to understand

that the benefits against what we are asking these election officials to do in an increasingly complex environment, that is also made more difficult by the constant need to provide factual information back out to voters. Right?

So, as decisions like this are made locally, it is our Federal system at work, a deep understanding of what are we asking election officials to do, how will they communicate with the public, what impact could this have on both the administration and confidence in the election process, is really, really critical because it is hard work. They have little resourcing and they are being asked to do more and more.

Mr. GARBARINO. Yes, and specifically, you know, municipal elections, the city council and the mayor only have control over the city council, but there are not just city council elections. I mean, there are Supreme Court seats that are up for election in New York. There are State Court seats, special elections to fill State and Congressional seats that are held in the off years—in the odd years. So, you know, what are the election officials going to have to do? Are they going to have to create separate ballots? I mean, what kind of, you know, process is this going to do and how confusing can it be?

Mr. MASTERSON. Yes, thank you, Ranking Member. I am not specifically familiar with all the language in the bill, but any time you are asking for sort-of a separate registration system, it increases, as you noted correctly, the complexity of what databases have to be administered, what the registration process looks like, and how you create that separation, and then how you are going to create ballots, ballot styles. I mean, depending on how the jurisdictions administer elections, you are talking about thousands of ballot styles and ensuring that the right people get the right ballot styles, all things that election officials are used to, but layering on these responsibilities is a challenge. When making changes like this, understanding the risks that are involved, understanding the responsibility and the additional burden that is being placed on the administrators is really important, so that they can do their job and succeed at it.

Mr. GARBARINO. I appreciate your answer. I know we focus on your role as an election official. Now I am going to ask a question about your role at the Election Assistance Commission.

In your report you recommended that Congress reforms the EAC and designated CISA as the technical lead for elections, which would allow the EAC to focus on its core mission of election administration. Can you walk us through how this would look in practice?

Mr. MASTERSON. Yes. So, I have obviously spent time at both agencies and believe deeply in the mission of both agencies, the EAC and CISA. Right now what you have is sort-of a muddy waters on sort-of the technical responsibilities with the EAC administering, for instance, the testing and certification program and voting systems, providing guidance through their clearinghouse.

What I would like to see, in order to save valued resources, I mean, the EAC is small and has limited resources, CISA much larger, but has a huge mission space, is to really say, OK, CISA, you are the technical lead. You worry about the cybersecurity, the

infrastructure, physical security, advice, and guidance. You support through the Elections Information Sharing and Analysis Center the sharing of threat and risk data. EAC, literally, you can now focus on everything else: Grant distribution, best practices around things like poll worker training, ballot layout. I mean, there is so much more.

So, CISA has the expertise. CISA is out with the election officials providing thousands of assessments, right, throughout the year and understands both the maturity, the cybersecurity maturity of these offices and the risk framework around them.

Mr. GARBARINO. I appreciate that. I know my time has expired, so I will yield back. Thank you, Mr. Masterson.

Mr. MASTERSON. Thank you, sir.

Chairwoman CLARKE. Thank you very much, Ranking Member. The Chair will now recognize other Members for questions they may wish to ask the witnesses. In accordance with the guidelines laid out by the Chairman and Ranking Member in their February 3 colloquy, I will recognize Members in order of seniority, alternating between the Majority and the Minority. Members are also reminded to unmute themselves when recognized for questioning.

The Chair recognizes for 5 minutes the gentlewoman from Texas, Congresswoman Sheila Jackson Lee.

Ms. JACKSON LEE. Madam Chair, if I could be delayed and yield to one of the other Members, please.

Chairwoman CLARKE. The gentlelady will yield at this time. I now recognize the gentleman from Rhode Island, Congressman Langevin, for 5 minutes.

Mr. LANGEVIN. Thank you, Madam Chair. I want to thank you for holding this important hearing. I want to thank our witnesses for their testimony and their insights, very helpful. If I could, I would like to start with Mr. Masterson.

Mr. Masterson, in your testimony you suggest a number of statutory baselines for State and local election offices and election vendors. What is your assessment right now of the current technical capacity of relevant State and local stakeholders to implement these kinds of cybersecurity measures? How can the Federal Government assist to build technical capacity where it is needed?

Mr. MASTERSON. Yes. Thank you, Representative. Thank you for your service and support for cybersecurity work and challenging us at CISA throughout the election on the work that we are providing and support we are providing election officials. I really appreciate it.

The current state is we have come a long way since 2016 and 2017 and the declaration of elections as critical infrastructure. We see more multi-factor authentication across election offices. We see more network segmentation and database security access controls in place. That bore out in 2020 with the security of the 2020 election.

But the reality is, as you know, sir, well, this is, you know, not something that you ever finish. Right? It is a constant and evolving process to secure the systems and on-going evolving threats.

So what CISA could do is really reach that last mile, those mid-to-small counties that have little to no IT support, that are doing the best that they can with the resources they have, and really

identify, No. 1, those baseline practices, get those in place; and then, No. 2, help them respond to emerging threats, like we have seen with things like SolarWinds or other vulnerabilities. Really push that information out and help them mitigate the vulnerabilities that may be present in their systems. The way to do that is utilizing their field forces in combination with something like Crossfeed, which proactively scans and looks for those types of vulnerabilities, so that they can alert those jurisdictions you have this, we are here to support.

Mr. LANGEVIN. Very helpful. Thanks for the insights into your work at CISA as well.

To all of our witnesses, I want to just turn to election software supply chain, if I could. Again, all of the witnesses, what capabilities do State and local entities currently have to evaluate the security of the software supply chain and voting infrastructure? Are there opportunities for Congress to support improvements to those capabilities?

If we could start with Ms. Ramachandran and then work our way down the line, that would be helpful.

Ms. RAMACHANDRAN. Thank you so much for your question. Unfortunately, State and local election officials don't have a Federal framework for security standards for election vendors to rely on to help them ensure that they are choosing vendors that are following best practices in terms of supply chain risk management. So, one helpful way for Congress to be helpful in this would be to either mandate or incentivize rigorous vendor security standards.

For instance, Congress could limit the use of Federal funds for elections to those vendors who agree to meet certain cybersecurity personnel and supply chain best practices. Those could be promulgated by CISA, for instance, with perhaps the assistance of the Election Assistance Commission. This would be one way to really sort-of help beef up and incentivize the choice of good vendors.

At the same time, States and counties can improve their procurement processes, negotiate for contracts in which vendors agree to mitigate supply chain risks.

Mr. LANGEVIN. Thank you. The next witness, if you could——

Mr. STAMOS. Yes. So, I will just say I think the supply chain issue is huge overall in cyber right now. I got pulled into the SolarWinds investigation. Against an adversary of that level, when you have got somebody as skilled as SVR attackers who are willing to spend 9 months or a year infiltrating the supply chain, I think it is extremely unlikely that we can ask either election manufacturers themselves or State and local officials to stand up against that level of adversary on their own.

So, I do think there needs to be a real aggressive move on collective defense here. I think a ISAC-like model of much more aggressive kind of openness by the manufacturers and willingness to work with one another and then to work with the FBI, CISA, NSA, Cyber Division, and such is going to be critical because against attackers like that it is an extremely difficult pull.

Mr. ROSENBERG. I defer to Ms. Ramachandran on this issue.

Mr. LANGEVIN. Thank you.

Mr. MASTERSON. Sir, the only other thing I would add is the assumption in elections that we shouldn't be reliant on the perform-

ance of or security of the software and hardware counting the votes, which is why paper ballots and post-election audits are so critical, that we have that check precertification to verify the results and to know that the votes were counted as cast, and so a continued focus. We have seen great improvement. As was noted, 96 percent of votes cast in this last election were on auditable paper ballots. A continued expansion of the use of those paper ballots and auditing them is critical to this.

Mr. LANGEVIN. Yes, I——

Chairwoman CLARKE. The Chair now recognizes for 5 minutes the gentlewoman from Tennessee, Mrs. Harshbarger.

Mrs. HARSHBARGER. Thank you, Madam Chair. Thank you witnesses here today. This question is for Mr. Masterson.

You know, numerous polls recently have shown that an overwhelming majority of Americans support common-sense election security measures, like voter ID laws, including 77 percent of Black voters, 78 percent of Hispanic voters. And many laws because of those things have enacted such laws to institute those voter IDs.

In your view, would Federal legislation that nullifies or undermines these popular State election security laws, like voter ID, increase or decrease election security, sir?

Mr. MASTERSON. Yes. Thank you, Representative. Voter confidence, as the research has shown, is a fickle mistress in that it is largely dependent on how your candidates faired in the prior election. So, for me, legislation, whether at the Federal, State, or local level, should be based on, No. 1, what information, what data can we provide to voters about the process to increase their understanding and confidence in the individual security of their vote? No. 2, what do State and local election officials need?

There is a reason and it is appropriate and it is good that State and locals run elections, so that they can engage directly with voters about the protections they put in place. What support, what information do they need in order to secure their process and go out and talk directly to their voters about the steps that they have taken?

So, for me, any legislation based in those principles is important.

Mrs. HARSHBARGER. Yes. Well, you know, cybersecurity, have you ever watched the documentary "Kill Chain" ?

Mr. MASTERSON. Yes.

Mrs. HARSHBARGER. OK. Tell me your thoughts on that when he delves into voter integrity and cybersecurity world.

Mr. MASTERSON. Yes. So, I am no movie critic, so I won't weigh in on the cinematic value, but I think "Kill Chain" and, frankly, work that we did at CISA with the security research community raises an important conversation about how do we talk about vulnerabilities in critical systems, whether that is voter registration, electronic poll books, election night reporting, or voting systems? How do we get that information in the hands of those who can fix it? Then how do we talk to voters about that?

Then, second, as I mentioned before, what resilience measures can we put in place such that if there is actually an exploitation of a vulnerability, we are able to recover? We are able to maintain the integrity of the process and ensure that voters know that their

voted was counted as cast. For me, a large part of that is post-election audits in the form of paper ballots precertification.

Mrs. HARSHBARGER. Absolutely. Well, ballot harvesting, what are your thoughts on that? Do you think Federal legislation that is proposed now that requires unlimited ballot harvesting in every State would reduce election integrity and security?

Mr. MASTERSON. So, each State has their own requirements, as you know, Representative, around how they manage the collection and security of ballots. Each State knows what they need to do to manage that. So, as I look at the security of our ballots, at the security of our votes, ensuring proper chain of custody, ensuring proper documentation of that as appropriate.

With that said, in my home State of Ohio we have had both early in-person voting and vote by mail for a number of years. The election officials have administered that with integrity and security. So, I have confidence in their professionalism, the bipartisan nature of the process to do that well.

Mrs. HARSHBARGER. Well, you know, at a press conference yesterday President Biden did say, he suggested there could be problems with the mid-term elections without voting rights legislation being passed by the Federal Government. So, therefore, you know, basically what he said was it could easily be illegitimate in the mid-terms coming up. You know, that sends a message now that maybe this won't be done properly with these election officials. What are your thoughts on what he said?

Mr. MASTERSON. Just as in 2020, where the election officials heroically performed in the face of a global pandemic, record turn-out, and challenges across the board, I have full faith and confidence in them. Would hope that nobody would use the question of the legitimacy of our elections for any, you know, purpose, and understand and work with those election officials to understand the steps they take to protect, like they did in 2020.

Mrs. HARSHBARGER. OK. Well, thank you, sir. Madam Chair, I yield back.

Mr. MASTERSON. Thank you.

Chairwoman CLARKE. Thank you. The Chair now recognizes for 5 minutes the gentlewoman from Texas, Ms. Sheila Jackson Lee.

Ms. JACKSON LEE. Thank you very much, Madam Chair. Thank you for an important hearing and important statement on the importance of voting integrity and security.

I do my questioning in the backdrop of a tragic and unfortunate action on the floor of the U.S. Senate when I think those who voted obviously misinterpreted their responsibilities in securing democracy. A part of that, of course, is the infrastructure. I want to begin the brief time that I have for my questions to at least note that the elections representative under the past administration clearly made sure that there was no fraud in the 2020 election of any sizable amount.

In addition, there was no fraud of any sizable amount indicated by the Republican secretary of state in the State of Texas. But yet, we have been the victims of a brutal scheme of purging voters, of establishing new crimes in voting, and a number of impediments to mail-in voting, impediments to early voting. So, even aside from

the infrastructure, we are rife with the challenges that we would have.

So, let me indicate for all witnesses, based upon the fatal attack on the U.S. Capitol on January 6 that demonstrated the very real potential for failed false narratives about stolen or rigged elections to incite real-time vigilance, I am sorry, violence in the weeks before January 6, former President Trump waged an outright, overt disinformation campaign explicitly designed to overturn the democratic will of the people.

To the persons on this panel, how have the events of January 6 and corresponding threats of attacks on other State capitals or to individual election officials changed the way you think about election misinformation? That is obviously technology and the Big Lie narrative. How might this narrative metastasize over the course of this year and before the Presidential election?

I would appreciate it if, starting with Ms. Gowri Ramachandran, if I have it right, starting with you, please, of Brennan Center, and then Alex, Ezra.

Ms. RAMACHANDRAN. Thank you so much for that question. It is interesting that you note that the misinformation and disinformation campaign led to violence on January 6, and asked about how it has metastasized. Since January 6, 2021, we have seen many election officials also being subject to threats of violence, harassment, real physical security risks. When Congress was counting the electoral votes on January 6, they were, in essence, acting as election administrators, as neutrally counting up the votes and declaring—you know, certifying the election.

So, I think it is really a continuous chain of threats of physical violence against those who are attempting to respect the will of the voters. It really amplifies the need for increased physical security protections for election administrators.

Mr. STAMOS. You——

Ms. JACKSON LEE. From——

Mr. STAMOS. I am sorry.

Ms. JACKSON LEE. Yes, just proceed. Also emphasize, thank you, the issue of disinformation technology that can also be threatening. Thank you.

Mr. STAMOS. Yes, Congresswoman. So, something that has changed and progressed since January 6 is the actions the major platforms took to finally enforce a bunch of rules that were on the books, but that were not aggressively enforced before January 6 has meant there has been a fracturing of the social media landscape upon which these things happen. So, we have a really significant growth of alternative platforms that are much more radical and that have almost no content moderation at all, as well as a move of a lot of this content to point-to-point messengers, most notably Telegram, which has both kind-of small group as well as more amplifying components to it.

So, the net effect of that is that our ability to understand what is going on is actually much reduced versus where we were in 2020 because most of these platforms have no official way to study them and we don't really have the legal frameworks in place to authorize either the Government or independent groups like our own to be

working on this, which is why we have been pushing for transparency legislation that I would love for Congress to take up.

Mr. ROSENBERG. I would just add one thing, Congresswoman Jackson Lee, and it really has to do with your State of Texas, which has this unfortunate history of intimidation against people of color when they are voting. S.B. 1, which is Senate Bill 1, which was passed this year gives partisan poll watchers virtually untrammeled access to polling places that will increase the opportunity for that kind of intimidation while, at the same time, it criminalizes any obstruction with the partisan poll workers by election judges. That, to me, is a very serious thing, particularly in light of the events of January 6.

Ms. JACKSON LEE. Those are really strong evidences of an attack on the election infrastructure and the cyber question, and I am grateful to the Chairwoman for this hearing, is out of control and will continue to be if we do not, as you have said, provide transparency and also some framework for the utilization during election periods.

Chairwoman CLARKE. The Chair now recognizes for 5 minutes——

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

Chairwoman CLARKE. The Chair now recognizes for 5 minutes the gentleman from Georgia, Mr. Clyde.

Mr. CLYDE. Thank you, Madam Chair. The statements that the November 2020 election was the most secure an election—a secure election in American history, that, in my opinion, is the Big Lie.

You know, that is what we heard in my own State of Georgia, but now we are finding out about massive ballot drop box stuffing, ballot harvesting happening between 2 a.m. and 5 a.m. in the morning. Who takes their ballot down and puts it in the drop box between 2 a.m. and 5 a.m. in the morning?

Where one person has admitted to being paid $45,000 to harvest 4,500 ballots. That is $10 a ballot. That is only one person. They brought evidence to indicate that over 240 people were involved. If they all harvested only 1,000 ballots each that would be over 240,000 ballots. The 2020 election is called the most secure in American history. No, I am sorry, but that is the Big Lie.

So, I have a couple of questions for you now. Ms. Ramachandran, do you believe that photo IDs used to verify voter identity increase election security? Just yes or no would be fine.

Ms. RAMACHANDRAN. No, I don't believe photo ID is necessary.

Mr. CLYDE. So, you don't believe that photo ID increases election security. OK, that is fine.

Mr. Alex Stamos, if you would tell me, do you believe that photo ID increases election security?

Mr. STAMOS. It is not really my area, sir. I am sorry, I don't have an opinion.

Mr. CLYDE. You don't have an opinion on voter identity, OK. All right.

Mr. Rosenberg, I believe, if I remember correctly, that you made a comment in your statement that you called photo ID discriminatory against people of color. So, do you believe that photo ID increase election integrity or election security, i.e., used to verify a voter identity?

Mr. ROSENBERG. Congressman, there is no evidence of in-person voter fraud, which is the only thing that voter ID protects against. In Texas——

Mr. CLYDE. OK. So, just yes or no. Yes or no is my question to you.

Mr. ROSENBERG. No, I do not believe it increases security because there is no evidence of in-person——

Mr. CLYDE. OK. All right, thank you. So, you are a no.

Mr. Masterson, do you believe that voter ID increases election security by verifying a voter's identity?

Mr. MASTERSON. So, each State has their own identification requirements for each part of the process, and I trust the State and local election officials to understand what they need to do.

Mr. CLYDE. OK. So, you don't have an opinion then?

Mr. MASTERSON. My—I mean, each State sets it and follows it and my opinion is that they understand what their voters need and how they have to secure the process for each part of the process.

Mr. CLYDE. OK. All right. OK. Well, that definitely tells me where each of the witnesses stand when it comes to voter ID. You know, we use Government-issued picture ID for many, many things to verify exactly who you are. I couldn't fly here without showing a valid picture ID to TSA at the airport. In fact, even to go eat now in Washington, DC, you have to have a valid picture ID and a vaccination card to show who you are and the fact that you are vaccinated. The No. 1 thing that our Constitution protects, and that is one person, one vote, and, you know, for folks not to think that voter ID is important is just stunning to me.

But, Mr. Masterson, during your time at CISA you spent most of it speaking directly to State and local election officials about their cybersecurity capabilities and what resources they need to secure their systems. So, what CISA services had the greatest positive effect on election security in your opinion?

Mr. MASTERSON. Yes, I appreciate the question, Representative. In my opinion, those services that we provide at no cost out to those mid-to-small counties, including some in your home State, that allow them to identify possible vulnerabilities in the systems and mitigate those vulnerabilities, so, cyber hygiene scans, penetration testing, Crossfeed, those types of services.

Then the biggest benefit that I think we provided was the establishment of an Information Sharing and Analysis Center, where all election officials have access to on-going threat and risk information.

Mr. CLYDE. OK. Are there any specific services that CISA should be looking to expand or end?

Mr. MASTERSON. Absolutely. I appreciate that, Representative.

The first is expanding Crossfeed both in scope and scale. So, scanning for additional connectivity, including working with voting system manufacturers to look on-line if voting systems are connected. The second is looking to expand remote incident response services and email security. How can they help support better email security working with State election officials? Because we see email as high-risk and exploited often in these mid-to-small counties.

Mr. CLYDE. OK. Thank you very much. I appreciate that. Madam Chair, I yield back.

Chairwoman CLARKE. Thank you. The Chair now recognizes for 5 minutes the gentlewoman from Michigan, Ms. Slotkin.

Ms. SLOTKIN. Thank you, Madam Chairwoman. Thanks to all our witnesses for joining us.

The thing I want to talk about is the threats of violence to our election officials. That is something that, I am from Michigan, it has just been the kind of thing that has really infected our electoral process and I fear is actually dissuading people for running for clerk, which means people are just not going to participate in upholding the democracy.

So, the example I have here is Tina Barton. She was a Republican-elected clerk in Michigan, in one of my bigger cities of Rochester Hills. She corrected like a clerical error in 2020 on election night. Leaders of her own party claimed that there had been widespread fraud in Michigan's elections, and they tried to pressure her into casting doubt on the results of Michigan's election.

She did the right thing. She literally got on camera and refused, publicly rebutting this disinformation. But then like the onslaught came. Right? Just by doing that, doing her job, her and her husband, who is a sheriff's deputy, began to receive death threats. They had to upgrade their own home security systems, thousands of dollars. After 8 years of serving Rochester Hills, she went on and now she is doing bigger and better things at the Election Assistance Commission.

But she is not alone. We have clerks from Lansing, Michigan. Chris Swope, he has received a number of death threats. It is just very common. The majority of the clerks in my area are Republican, so this isn't like a partisan, you know, thing.

So, I just—I would love maybe, Mr. Masterson, starting with you, you have laid out some things that CISA and DOJ can do to protect election workers, but just tell us what works. Like what actually works to protect the people at the ground level who are on the receiving end of this vitriol?

Mr. MASTERSON. Yes. Thank you, Representative.

Accountability works. We need to see those who are threatening election officials, their families, workers, private industry workers in elections, we need to see them held accountable. We have seen surprising little indictments or enforcement against these folks. So, it starts with accountability.

Then second, additional resources, allowing these election officials, for instance, and judges, law enforcement officers get this benefit in many States, but protecting their personal information. Right? So, there are laws that could be passed to ensure that doxing is at least difficult or hard to do against these folks.

So, those are the two things that I think of immediately that would help.

Ms. SLOTKIN. Great. Then I think maybe for you and Mr. Stamos, you know, I have this—we are all talking about how to make sure that our kids know what is real information and what is disinformation. I hear all the time from moms like how hard it is to tell their kids where they can reliably get information and

how to teach them. So, I have this—I have a bill on digital literacy for kids.

Again, what works? Like what actually—what are the tools that I should be telling moms to use to help their kids, you know, tell fact from fiction? Mr. Stamos, do you want to start?

Mr. STAMOS. Sure. So, you know, I mean, for the work I do, when we talk about kids, I think a key thing to work with your kids is who they are interacting with on-line and to keep kind-of a presence in their on-line browsing experience. I think there is way too many, you know, I am a parent of 3. It is really easy for us to give our kids kind-of free range and access. That is both risky from kind-of an interpersonal perspective and some of the things that happen to kids when they run into bad folks on-line, but then also their consumption of information. You know, my sons watch a lot of YouTube and there are a lot of videos there that aren't so accurate, and we have to have discussions about it.

So, I think just being part of your kid's life and being—looking over their shoulders is a big thing.

The other issues really are parents, for those of us in this rough age range, and that is when we talk about the disinformation around elections and such, there is actually a real issue about older folks there. For that I don't have any good solutions.

Ms. SLOTKIN. Mr. Masterson, any quick comments?

Mr. MASTERSON. Yes, just the other thing is establishing the trusted sources, the trusted voices. Secretary Benson in Michigan has done a tremendous job with this, pushing out factual information about the elections. But then we need amplifiers, those trusted voices in communities, including getting kids involved. We know there are lots of opportunities at the State and local level across the United States for kids to serve as poll workers or to volunteer, depending on age. So, how do we get them into the elections process, into our democracy early, so that they can understand how it works, have more confidence, and be participants as they reach voting age?

Ms. SLOTKIN. Great. Thank you, Madam Chair. My time is up. I yield back.

Chairwoman CLARKE. Thank you. With that, I would like to thank our expert witnesses for their valuable testimony and the Members for your questions today. There is still a lot more to unpack in this space. I want to thank the Ranking Member for his partnership in, you know, this endeavor.

Let me just say that the Members of the subcommittee may have additional questions for the witnesses. I ask that you respond expeditiously and in writing to those questions. The Chair reminds Members that the subcommittee record will remain open for 10 business days.

Without objection, the subcommittee today stands adjourned. Everyone stay safe and stay healthy.

[Whereupon, at 3:18 p.m., the subcommittee was adjourned.]

○