AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PREPARING FOR 2020: HOW ILLINOIS IS SECURING ELECTIONS

FIELD HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

OCTOBER 15, 2019

Serial No. 116–40

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

40–456 PDF WASHINGTON : 2020

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
CEDRIC L. RICHMOND, Louisiana
DONALD M. PAYNE, JR., New Jersey
KATHLEEN M. RICE, New York
J. LUIS CORREA, California
XOCHITL TORRES SMALL, New Mexico
MAX ROSE, New York
LAUREN UNDERWOOD, Illinois
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
NANETTE DIAZ BARRAGÁN, California
VAL BUTLER DEMINGS, Florida

MIKE ROGERS, Alabama
PETER T. KING, New York
MICHAEL T. MCCAUL, Texas
JOHN KATKO, New York
MARK WALKER, North Carolina
CLAY HIGGINS, Louisiana
DEBBIE LESKO, Arizona
MARK GREEN, Tennessee
VAN TAYLOR, Texas
JOHN JOYCE, Pennsylvania
DAN CRENSHAW, Texas
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina

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

CONTENTS

PREPARING FOR 2020: HOW ILLINOIS IS SECURING ELECTIONS

Tuesday, October 15, 2019

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Gurnee, IL.

The committee met, pursuant to notice, at 10:08 a.m., in the Village of Gurnee Council Chambers, Gurnee Village Hall, 325 N. O'Plaine Road, Gurnee, Illinois, Hon. Bennie G. Thompson (Chairman of the committee) presiding.

Present: Representatives Thompson and Underwood.

Also present: Representative Casten.

Chairman THOMPSON. The Committee on Homeland Security will come to order.

I ask unanimous consent that Mr. Casten be permitted to participate in today's hearing. Without objection.

Good morning. Let me apologize for my accent. I am from Mississippi.

[Laughter.]

Chairman THOMPSON. It gives everybody consternation because they say I haven't heard somebody talk like that in a long time. So trust me, the speed of my voice has nothing to do with my brain.

[Laughter.]

Chairman THOMPSON. I am absolutely proud to be here. As I said to Congresswoman Underwood earlier, I spent the summers of my college education in Chicago, Illinois working because that is how I was able to finance my college education in Mississippi because Illinois paid far better wages than Mississippi.

So I have come back and I thank you for making me what I am today because of your generosity.

But I would also like to thank Chairman—Vice Chair Underwood for inviting committee Members to Illinois to hear State and local perspectives on election security.

Since she arrived in Congress in January, the Vice Chair has demonstrated a strong commitment to raising the bar on Federal efforts to improve election security at the State and local level.

Too often well-intentioned officials in Washington do not have a complete understanding of how the Federal Government can best assist State and local officials in their mission.

But Ms. Underwood has fought to make sure that the boots on the ground have the resources they need and a seat at the table, which is why we are having this field hearing today.

The Vice Chair has been a valued leader on the Homeland Security Committee, and on election security in particular I want to thank her for her continued efforts to hold the folks in Washington accountable on behalf of her constituents.

Election security requires a whole-of-government approach—Federal, State, and local—effort to protect America's elections. It is a National security issue that transcends party politics and reaches into the heart of our democracy.

As we approach the 2020 elections it is critical that we work together to protect democracy's most sacred tradition: Free and fair elections.

Last Congress, I co-chaired the Congressional Task Force on Election Security and met with election security experts, State election officials, and National security experts to assess vulnerabilities in election infrastructure and determine how to address them.

The task force published a report in February 2018 that included 10 recommendations and introduced legislation to implement them.

That legislation, Election Security Act, was included in H.R. 1, the For the People Act, which passed the House in March of this year.

Unfortunately, the Senate has yet to act on that or any other meaningful election security legislation. Nevertheless, since 2016 progress has been made toward more secure elections at State and local levels.

The Department of Homeland Security and Election Assistance Commission have built stronger, more effective partnerships with State and local officials.

States like Illinois are at the forefront of that effort and have led the way. From improvements in the Illinois Century Network to the Cyber Navigator Program, the State has made smart investments in election security capabilities that makes it harder for adversaries to meddle in the 2020 elections.

But continued election security efforts cost money and I imagine that State and local election officials here struggle with the same budget demands as their counterparts do in my district in Mississippi.

That is why I am glad to be here today to learn from all of you what you need from us to help you continue the important work you do to secure elections. The Federal Government, especially Congress, must understand the resource constraints of local election officials and partner with them to address vulnerabilities to election infrastructure through grants and services.

Local election officials are on the front line of securing our elections and your success depends on the resources and support you receive from Federal and State government.

The intelligence community has made clear the threats to our elections persist. Acting Director of National Intelligence Joseph Maguire told Congress that we should expect adversaries and strategic competitors to refine their capabilities and add new tactics as they learn from each other's experiences in advance of the 2020 elections.

I look forward to hearing from our panel of witnesses today about how Illinois is leading the way in securing their election critical infrastructure and how Congress and Federal agencies can support

these efforts to further strengthen our elections and protect them from another attack.

Before I close, I would like to thank the good people of Gurnee Village Hall for hosting today's hearing.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

OCTOBER 15, 2019

I would like to thank the committee's Vice Chair, Ms. Underwood, for inviting committee Members to Illinois to hear State and local perspectives on election security. Since she arrived in Congress in January, the Vice Chair has demonstrated a strong commitment to raising the bar on Federal efforts to improve election security at the State and local level. Too often, well-intentioned officials in Washington do not have a complete understanding of how the Federal Government can best assist State and local officials in their mission. But Ms. Underwood has fought to make sure the boots on the ground have the resources they need and a seat at the table, which is why we are having this field hearing today. The Vice Chair has been a valued leader on the Homeland Security Committee, and on election security in particular, and I want to thank her for her continued efforts to hold the folks in Washington accountable on behalf of her constituents.

Election security requires a whole-of-government, Federal, State, and local, effort to protect America's elections. It is a National security issue that transcends party politics and reaches to the heart of our democracy. As we approach the 2020 election, it is critical that we work together to protect democracy's most sacred tradition: Free and fair elections. Last Congress, I co-chaired the Congressional Task Force on Election Security, and met with election security experts, State election officials, and National security experts to assess vulnerabilities in election infrastructure and determine how to address them. The Task Force published a report in February 2018 that included 10 recommendations and introduced legislation to implement them. That legislation, the Election Security Act, was included in H.R. 1, the For the People Act, which passed the House in March of this year. Unfortunately, the Senate has yet to act on that or any other meaningful election security legislation.

Nevertheless, since 2016, progress has been made toward more secure elections at the State and local level. The Department of Homeland Security and Election Assistance Commission (EAC) have built stronger, more effective partnerships with State and local election officials. And States like Illinois are at the forefront of that effort and have led the way. From improvements to the Illinois Century Network to the Cyber Navigator Program, the State has made smart investments in election security capabilities that make it harder for adversaries to meddle in the 2020 election. But continued election security efforts cost money, and I imagine that State and local election officials here struggle with the same budget demands as their counterparts in my District in Mississippi. That is why I am glad to be here today to learn from all of you what you need from us to help you continue the important work you do to secure elections. The Federal Government—especially Congress—must understand the resource constraints of local election officials and partner with them to address vulnerabilities to election infrastructure though grants and services.

Local election officials are on the front lines of securing our elections, and your success depends on the resources and support you receive from Federal and State governments. The intelligence community has made clear the threats to our elections persist. Acting Director of National Intelligence, Joseph Maguire, told Congress that we should expect "adversaries and strategic competitors to refine their capabilities and add new tactics as they learn from each other's experiences" in advance of the 2020 elections. I look forward to hearing from our panel of witnesses today about how Illinois is leading the way and securing their critical election infrastructure, and how Congress and Federal agencies can support these efforts to further strengthen our elections and protect them from another attack.

Chairman THOMPSON. With that, I yield back the balance of my time and I now recognize the Vice Chair of the full committee, the gentlewoman from Illinois, Ms. Underwood, for an opening statement.

Ms. UNDERWOOD. Thank you, Mr. Chairman.

Good morning. Thank you all so much for being here with us today. As Vice Chair of the House Committee on Homeland Security, I am so thrilled that you joined us as we gaveled in this committee's first-ever hearing in the Illinois 14th Congressional District.

I would like to also thank the village of Gurnee for hosting the committee's hearing today and my colleague, Congressman Casten, for taking part in the hearing. Thank you.

I would also like to thank Chairman Thompson for holding this hearing and joining us all the way from Mississippi, and thank you to the panel of experts who—and public servants assembled here today. I appreciate the important work that you do and I look forward to hearing from each of you.

I would also like to acknowledge the Members of our community who have made time to join us for this important conversation and an extra special thank you to Mr. Jacob Carlton and his AP Government students that are here from Zion-Benton Township High School. Thank you for being here today.

In February of this past year, this committee, led by Chairman Thompson, held its first hearing of the 116th Congress on defending our democracy by protecting and security our Nation's elections.

U.S. intelligence officials have confirmed that there was foreign interference in the 2016 elections. In Illinois, this resulted in foreign actors accessing the records of 76,000 Illinois voters.

Since then, State and local election officials have been working hard to improve election systems and infrastructure. But due to limited resources, some have faced challenges to upgrading legacy machines and bringing on additional cybersecurity personnel.

Congress has recognized the challenges that come with improving decades-old infrastructure and have provided critical funding and assistance to States since our State was hacked in 2016.

Here in Illinois, State and local election officials have worked together to implement a world class Cyber Navigator Program to help the State improve its cybersecurity posture and to mitigate future attacks.

This program has allowed our State to hire additional cybersecurity personnel to facilitate information sharing and provide guidance on best practices to each of the 108 election authorities in Illinois.

The Cyber Navigator Program is a valuable tool for the election officials here in Illinois and it is my hope that programs such as this can serve as models for other States.

In addition to the funding provided by Congress, this committee has made election security a priority and has put forward tough broad policies to secure our elections.

I am proud that these policies were included in H.R. 1, the For the People Act, which we passed in the House in March.

This is an important package of reforms because it seeks to restore integrity in our Government and ensure that each and every American can fully participate in our democracy.

Specifically, it helps protect U.S. elections by improving voting system security by requiring the Department of Homeland Security to maintain election systems as critical infrastructure.

It also requires regular testing of voting systems and provides much-needed resources for States to conduct post-election audits and upgrade legacy election systems.

I was also proud to support the fiscal year 2020 House Appropriations package which included $600 million for the Election Assistance Commission to distribute election security grants to bolster State election security efforts.

These two House-passed measures go a long way to help districts like this one, which is operating under a constrained budget while trying to do the absolute most to ensure the integrity of our elections.

Now, the 2020 election is right around the corner and adversaries are already working to interfere. We don't have time to wait. The Senate should immediately pass legislation to strengthen our election security.

As the Chairman stated in our previous election security committee hearing, we have made great strides since 2016. But we must remain vigilant against bad actors working to undermine the beacon of American democracy.

I hope our discussion today will provide this committee and the public with valuable information and resources and assistance in preparation for the upcoming elections in 2020.

The integrity of our elections is essential to the preservation of our republic and it is our patriotic duty as Americans and my sacred duty as someone elected to represent this beautiful community, the Illinois 14th, to ensure that our elections are free from foreign interference.

I look forward to hearing from the witnesses today on the progress that has been made here in Illinois, what additional work we can do to support our State and local election officials, and how we can help other States use Illinois' success as a model for their own programs.

Thank you again for being here today. I am looking forward to an educational and productive hearing, and I yield back.

[The statement of Honorable Underwood follows:]

STATEMENT OF HONORABLE LAUREN UNDERWOOD

OCTOBER 15, 2019

Good morning, welcome, and thank you all so much for being here today!

As vice chair of the House Committee on Homeland Security, I am so thrilled you joined us as we gavel in this committee's first-ever hearing in Illinois's 14th Congressional District.

I would like to thank the Village of Gurnee for hosting the committee's hearing today and my colleague, Representative Casten, for taking part in today's hearing.

I would also like to thank Chairman Thompson for holding this hearing and for joining us all the way from Mississippi.

Thank you to the panel of experts and public servants assembled today. I appreciate the important work you do, and I look forward to hearing from each of you.

I would also like to acknowledge the members of our community who have made time to join us for this important conversation . . . and a special thank you to Mr. Jacob Carlson and his AP Government students from Zion Benton Township High School for being here today.

In February of this year, this committee, led by Chairman Thompson, held its first hearing of the 116th Congress on defending our democracy by protecting and securing our Nation's elections.

U.S. intelligence officials have confirmed there was foreign interference in the 2016 elections. In Illinois, this resulted in foreign actors accessing the records of 76,000 Illinois voters.

Since then, State and local election officials have been working hard to improve election systems and infrastructure, but due to limited resources, some have faced challenges in upgrading legacy machines and additional hiring of cybersecurity personnel.

Congress has recognized the challenges that come with improving decades-old election infrastructure and has provided critical funding and assistance to States since our State was hacked in 2016.

Here in Illinois, State and local election officials have worked together to implement the world-class Cyber Navigator Program to help the State improve its cybersecurity posture and mitigate future attacks.

This program has allowed the State to hire additional cybersecurity personnel to facilitate information sharing and provide guidance on best practices to each of the 108 election authorities in Illinois.

The Cyber Navigator Program is a valuable tool for the election officials in my State, and it is my hope that programs such as this one can serve as a model for other States.

In addition to funding provided by Congress, this committee has made election security a priority and has put forward tough, broad policies to secure our elections. I'm proud that these policies are included in H.R. 1, the For the People Act, which we passed in the House in March of this year.

This is an important package of reforms because it seeks to restore integrity in Government and ensure each and every American can fully participate in our democracy.

Specifically, it helps protect U.S. elections by improving voting system security by requiring the Department of Homeland Security to maintain election systems as critical infrastructure, require regular testing of voting systems, and provide resources for States to conduct post-election audits and upgrade legacy election systems.

I also was proud to support the fiscal year 2020 House appropriations package, which included $600 million for the Election Assistance Commission to distribute Election Security Grants to bolster State election security efforts.

These 2 House-passed measures go a long way to help districts like this one, which is operating under constrained budgets while trying to do the absolute most to ensure the integrity of our elections.

The election is right around the corner and adversaries are already working to interfere. We do not have time to wait. The Senate should immediately pass legislation to strengthen our election security.

As the Chairman stated in our previous election security committee hearing, we have made great strides since 2016, but we must remain vigilant against bad actors working to undermine the beacon of American democracy.

I hope our discussion today will provide this committee and the public with valuable resources and assistance in preparation for the upcoming elections in 2020.

The integrity of our elections is essential to the preservation of our republic, and it is our patriotic duty as Americans, and my sacred duty as someone elected to represent this community, to ensure our elections are free from foreign interference.

I look forward to hearing from the witnesses today on the progress that has been made in Illinois, what additional work we can do to support our State and local election officials, and how we can help other States use Illinois's successes as a model for their own programs.

Thank you again to everyone for being here today—I'm looking forward to an educational and productive hearing.

Chairman THOMPSON. I thank the gentlewoman.

Other Members of the committee are reminded that under the committee rules opening statements may be submitted for the record.

I would like to extend a welcome to our witnesses.

Mr. Matthew Masterson is a senior advisor on election security at the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security, commonly referred to as CISA. Prior to that, he served as chairman of the Election Assistance Commission.

Mr. Steve Sandvoss, executive director of the Illinois Board of Elections, Mr. Sandvoss previously served as the Board of Elections' general counsel and has worked for the State Board of Elections for over 30 years. Congratulations.

Ms. Robin O'Connor is a clerk for Lake County, Illinois. Ms. O'Connor has been in public service for nearly 13 years. Thank you.

Finally, Ms. Elizabeth Howard is counsel for the Brennan Center for Justice's Democracy Program. Ms. Howard focuses her work on cybersecurity in elections.

Prior to that, Ms. Howard served as deputy commissioner for the Virginia Department of Elections.

Without objections, the witnesses' full statement will be inserted in the record. I now ask each witness to summarize his or her statement for 5 minutes, beginning with Mr. Masterson.

STATEMENT OF MATT MASTERSON, SENIOR CYBERSECURITY ADVISOR, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, DEPARTMENT OF HOMELAND SECURITY

Mr. MASTERSON. Thank you, Chairman Thompson, Vice Chair Underwood, Congressman Casten.

Good morning and thank you for the opportunity to testify regarding the Department of Homeland Security's efforts to help secure our election infrastructure in Illinois and across this country.

My name is Matt Masterson. I am the election security lead for DHS and the previous chair of the U.S. Election Assistance Commission as well as election official in the State of Ohio.

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, or CISA, has a strong relationship with State and local officials in Illinois.

The Department regularly engages with Illinois State Election Task Force on Training, assessment requests, and information sharing, and today I want to commend the 108 Illinois election districts and the State of Illinois for becoming members of the Election Infrastructure, Information Sharing and Analysis Center, or EIISAC.

In doing so, all election districts in Illinois are part of a robust community sharing actionable information and valuable alerts and warnings.

I also want to commend Illinois' successful Cyber Navigator Program that has been mentioned, which is truly a model for the rest of the country to follow.

Our progress in working with Illinois is reflective of our progress with the election community across the country. CISA's mission is clear, to support election officials and their private-sector partners to manage—to identify and manage risk to their systems, help them manage a response within the existing constitution and election traditions.

Elections are run at the State and local level by dedicated professionals across America's more than 8,800 election jurisdictions. But those officials shouldn't have to defend themselves from sophisticated and persistent threats on their own.

Since 2016, we at CISA have learned a lot. Over the last 2 years we have worked tirelessly to strengthen our partnership with the election community.

For the 2020 election we are already providing voluntary resources and services to all 50 States, over 2,000 local jurisdictions, 6 election associations, and 12 election vendors.

Our approach is threefold: No. 1, making sure the election community has the information they need to defend their systems; No. 2, making sure they have the technical support and tools they need to manage risk to their systems; and No. 3, building enduring partnerships to advance security efforts together.

CISA is focused on building scalable repeatable mechanisms to dramatically grow our information-sharing capabilities.

We share contextualized threat intelligence and actual information through the EIISAC with our close partners in the intelligence community and law enforcement and private sector.

More importantly, State and local officials across the country are sharing what they are seeing on their networks and on their systems with us.

We have deployed intrusion detection capabilities, or Albert sensors, to provide real-time detection capabilities of malicious activity on election infrastructure across all 50 States.

Second, we provide technical support and services to election officials and their vendors. Initially, we offered the standard services including vulnerability assessments that we offer to other Federal agencies and critical infrastructure partners.

As we refined our understanding of election officials' requirements, we shifted capabilities that are quicker, less intrusive, and can scale to more jurisdictions.

For instance, in 2018 and in 2019 we deployed a remote penetration testing capability thanks in part to the funding that Congress provided to us to allow for remote penetration of election systems, allowing us to identify risks and vulnerabilities in election systems without having to deploy teams into local election offices, interrupting both their time and people.

This scalability is critical because while our initial efforts in 2018 were primarily targeted at State election officials, we recognize the need to increase our support to counties and municipalities who operate elections as well.

Our Last Mile Initiative seeks to provide information customized to local county election officials. This initiative provides no-cost tailored information on cyber risks and a checklist of cybersecurity action items specific to them.

The final area of focus has been on building enduring partnerships toward collective defense. It may seem mundane, but governance, communications, coordination, training, and planning are critical foundational elements of our efforts to secure the Nation's elections.

We are clear-eyed that the threat to our democratic institutions remain and we must continue to press for increased security and resilience of our election systems.

For the 2020 election cycle, CISA has built off the lessons learned form 2018 and we are working to prioritize the following lines of effort.

No. 1, CISA is focused on expanding engagement at the local level. We continue to work with election officials to improve both their and our understanding of risks to election systems.

For instance, in June of this year we did our second annual tabletop vote exercise where 47 States, thousands of local officials, private sector, and the Federal Government worked together to work through scenarios, share information, and understand how we would respond collectively to threats to our election infrastructure.

No. 2, CISA has expanded our level of engagement and sharing of best cybersecurity practices with political organizations, including the DNC and RNC.

CISA recently joined the FBI and ODNI in offering briefings to Presidential campaigns registered with the FEC and is engaged directly with Presidential campaigns to offer services and share information.

No. 3, CISA, in coordination with our interagency partners, is committed to helping Americans recognize and avoid foreign disinformation operations impacting our elections.

Through innovative efforts like the war on pineapple campaign we were educated on the—we educated on the tactics of foreign influence using a topic everyone can relate to, the divisive issue of pineapple on pizza.

DHS is also working closely with the intelligence community to increase the quantity, quality, and timeliness of intelligence and analysis production at the Unclassified level to help election officials and the public identify foreign influence information.

We at CISA are committed to working with Congress to ensure our efforts cultivate a safer, more secure and resilient election.

Once again, thank you for the opportunity to appear before you and I look forward to your questions today.

Thank you very much for the time.

[The prepared statement of Mr. Masterson follows:]

PREPARED STATEMENT OF MATTHEW MASTERSON

OCTOBER 15, 2019

Chairman Thompson, Congresswoman Underwood, and Members of the committee, thank you for the opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) progress in reducing and mitigating risks to our Nation's election infrastructure. DHS has worked to establish trust-based partnerships with State and local officials who administer our elections, as well as political parties and campaigns, and I look forward to sharing with you an update on our work during the 2018 midterm elections and our priorities through the 2020 election cycle.

Leading up to the 2018 midterms, DHS worked hand-in-hand with Federal partners, State and local election officials, and private-sector vendors to provide them with information and capabilities to enable them to better defend their infrastructure. On the Federal level, DHS has coordinated closely with the Federal Bureau of Investigation (FBI), the Office of the Director of National Intelligence (ODNI), and Department of Defense (DOD) on these efforts. This partnership led to a successful model that we aim to continue and improve upon in the 2020 election cycle.

Since 2016, DHS's Cybersecurity and Infrastructure Security Agency (CISA) has led a voluntary partnership of Federal Government and election officials who regularly share cybersecurity risk information. CISA has engaged directly with election officials—coordinating requests for assistance, risk mitigation, information sharing, and incident response. To ensure a coordinated approach to assisting election officials protect the election infrastructure they manage, CISA has convened stakeholders from across the Federal Government through CISA's Election Security Initiative.

CISA and the Election Assistance Commission (EAC) have convened Federal Government and election officials regularly to share cybersecurity risk information and to determine an effective means of assistance. Since 2017, the Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) has worked to establish goals and objectives, to develop plans for the EIS partnership, and to create an EIS Sector-Specific Plan. Participation in the council is voluntary and does not change the fundamental role of State and local jurisdictions in overseeing elections.

CISA and the EAC have also worked with election equipment and service vendors to launch, in 2017, an industry-led Sector Coordinating Council (SCC), a self-organized, self-run, and self-governed council with industry leadership designated by SCC members. The SCC serves as the industry's principal entity for coordinating with the Federal Government on critical infrastructure security activities related to sector-specific strategies. This collaboration is conducted under CISA's authority to provide a forum in which Federal and private-sector entities can jointly engage in a broad spectrum of activities to coordinate critical infrastructure security and resilience efforts, which is used in each of the critical infrastructure sectors established under Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience.* The SCC has helped CISA further its understanding of the systems, processes, and relationships particular to operation of the EIS.

Within the context of today's hearing, I will address our efforts in 2018 to help enhance the security of elections that are administered by jurisdictions around the country, along with our election-related priorities through 2020. While there was activity targeting our election infrastructure leading up to the midterms, this activity was consistent with typical malicious activity targeting networked IT systems. DHS along with the Department of Justice (DOJ), "concluded that there is no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political/campaign infrastructure used in the 2018 midterm elections used for the U.S. Congress."[1]

ASSESSING THE THREAT

The Department, with and through DHS's Office of Intelligence and Analysis, regularly coordinates with the intelligence community and law enforcement partners on potential threats to the homeland. Among non-Federal partners, DHS has engaged with State and local officials, as well as relevant private-sector entities, to assess the scale and scope of malicious cyber activity potentially targeting election infrastructure in the United States. Election infrastructure includes the information and communications technology, capabilities, physical assets, and technologies that enable the registration and validation of voters; the casting, transmission, tabulation, and reporting of votes; and the certification, auditing, and verification of elections. Since 2016, State and local election offices and their private-sector partners have robustly shared information with DHS regarding activity targeting their systems. As with all networked IT systems, officials are seeing scanning and probing of their networks on a daily basis. Election infrastructure is a target for nation-state and non-state actors seeking access to systems containing sensitive data or what they perceive to be valuable information. DHS and our intelligence community (IC) partners continue to assess that the 2020 election remains a likely cyber and influence target for our adversaries. In short, the threat to our elections remains and it is incumbent on all levels of government to work together to respond.

ENHANCING SECURITY

During the 2018 midterms, CISA provided a coordinated response from DHS and its Federal partners to plan for, prepare for, and mitigate risk to election infrastructure. Working with election infrastructure stakeholders was essential to ensuring a more secure election. CISA and our stakeholders increased awareness of potential vulnerabilities and provided capabilities to enhance the security of U.S. election infrastructure, and shared best practices with other nations facing similar threats.

Election officials across the country have a long-standing history of working both individually and collectively to reduce risks and ensure the integrity of their elections. In partnering with these officials through both new and on-going engagements, CISA will continue to provide free, voluntary, prioritized services to support their efforts to secure elections in the 2020 election cycle.

---

[1] "Acting Attorney General and Secretary of Homeland Security Submit Joint Report on Impact of Foreign Interference on Election and Political/Campaign Infrastructure in 2018 Elections." February 5, 2019. Retrieved from: *https://www.dhs.gov/cisa/news/2019/02/05/acting-attorney-general-and-secretary-homeland-security-submit-joint-report*.

IMPROVING COORDINATION WITH STATE, LOCAL, TRIBAL, TERRITORIAL, AND PRIVATE-SECTOR PARTNERS

Increasingly, the Nation's election infrastructure leverages information technology for efficiency and convenience, but also exposes systems to cybersecurity risks, just like in any other enterprise environment. Similar to other sectors, CISA helps systems owners and operators in Federal departments and agencies, State, local, Tribal, and territorial (SLTT) governments, and the private sector to manage these cybersecurity risks. Consistent with our long-standing partnerships with State and local governments, we have been working with election officials to share information about cybersecurity risks, and to provide voluntary resources and technical assistance to manage those risks.

WORKING WITH THE EI–ISAC

CISA works with the Elections Infrastructure Information Sharing and Analysis Center (EI–ISAC) to provide threat and vulnerability information to State and local officials. Through funding by CISA, the Center for Internet Security created and continues to operate the EI–ISAC. The EI–ISAC has representatives co-located with CISA's operations center to enable regular collaboration and access to information and services for election officials.

PROVIDING TECHNICAL ASSISTANCE AND SHARING INFORMATION

Knowing what to do when a security incident happens—whether physical or cyber—before it happens is critical. CISA supports election officials with incident response planning including participating in exercises and reviewing incident response playbooks. Crisis communications is a core component of these efforts, ensuring officials are able to communicate transparently and authoritatively when an incident unfolds. In some cases, we do this directly with State and local jurisdictions. In others, we partner with outside organizations. We recognize that securing our Nation's systems is a shared responsibility, and we are leveraging partnerships to advance that mission. CISA actively promotes a range of services including:

Cyber hygiene service for internet-facing systems.—Through this automated, remote scan, CISA provides a weekly report identifying vulnerabilities and mitigation recommendations to improve the cybersecurity of systems connected to the internet, such as on-line voter registration systems, election night reporting systems, and other internet-connected election management systems.

Risk and vulnerability assessments (both on-site and remote).—We have prioritized State and local election systems upon request, and increased the availability of risk and vulnerability assessments. These in-depth, on-site or remote evaluations include a system-wide understanding of vulnerabilities, focused on both internal and external systems. We provide a full report of vulnerabilities and recommended mitigations following the testing.

Incident response assistance.—We encourage election officials to report suspected malicious cyber activity to CISA. Upon request, the CISA can provide assistance in identifying and remediating a cyber incident. Information reported to CISA is also critical to the Federal Government's ability to broadly assess malicious attempts to infiltrate election systems. This technical information will also be shared with other State officials so they have the ability to defend their own systems from similar malicious activity.

Information sharing.—CISA maintains numerous platforms and services to share relevant information on cyber incidents. Election officials may also receive information directly from CISA. CISA also works with the EI–ISAC, allowing election officials to connect with the EI–ISAC or their State Chief Information Officer to rapidly receive information they can use to protect their systems. Best practices, cyber threat information, and technical indicators, some of which had been previously Classified, have been shared with election officials in thousands of State and local jurisdictions. CISA incorporates privacy and civil liberties considerations and protections into the design of all its activities. Information sharing and use of cybersecurity threat indicators, or information related to cybersecurity risks and incidents complies with applicable lawful restrictions on its collection and use and with Federal and DHS policies protective of privacy and civil liberties.

Classified information sharing.—To most effectively share information with all of our partners—not just those with security clearances—DHS and its Office of Intelligence and Analysis (I&A) work with the intelligence community to rapidly declassify relevant intelligence or provide as much intelligence as possible at the lowest classification level possible. While DHS prioritizes declassifying information to the greatest extent possible, DHS also provides Classified information to cleared stake-

holders, as appropriate. DHS has been working with State chief election officials and additional election staff in each State to provide them with security clearances. These clearances have helped enable I&A and the intelligence community to deliver a number of Classified in-person and secure video teleconferences for a broad audience of State and local elections officials, in the lead-up to the 2018 midterms and into 2019.

Field-based cybersecurity advisors and protective security advisors.—CISA has cybersecurity and protective security personnel available to provide actionable information and connect election officials to a range of tools and resources to improve the cybersecurity preparedness of election systems, and to secure the physical site security of voting machine storage and polling places. These advisors are also available to assist with planning and incident management for both cyber and physical incidents.

Physical and protective security tools, training, and resources.—CISA provides guidance and tools to improve the security of polling sites and other physical election infrastructure. This guidance can be found at *www.dhs.gov/hometown-security.* This guidance helps to train administrative and volunteer staff on identifying and reporting suspicious activities, active-shooter scenarios, and what to do if they suspect an improvised explosive device.

ELECTION SECURITY EFFORTS LEADING UP TO THE 2018 MID-TERMS

In the weeks leading up to the 2018 midterm elections, CISA officials supported a high degree of preparedness Nation-wide. CISA provided free technical cybersecurity assistance, continuous information sharing, and expertise to election offices and campaigns. All 50 States, over 1,500 local and territorial election offices, 6 election associations, and 12 election venders were engaged in information sharing and receipt of assistance from EI–ISAC.

In August 2018, CISA hosted a "Tabletop the Vote" exercise, a 3-day, first-of-its-kind exercise to assist our Federal partners, State and local election officials, and private-sector vendors in identifying best practices and areas for improvement in cyber incident planning, preparedness, identification, response, and recovery. Through tabletop simulation of a realistic incident scenario, exercise participants discussed and explored potential impacts to voter confidence, voting operations, and the integrity of elections. Partners for this exercise included 44 States and the District of Columbia; EAC; Department of Defense, including the Office of the Secretary of Defense, U.S. Cyber Command, and the National Security Agency; DHS I&A; DOJ, including the Federal Bureau of Investigation; Office of the Director of National Intelligence; and National Institute of Standards and Technology (NIST).

Through the "Last Mile Initiative," CISA worked closely with State and local governments to outline critical cybersecurity actions that should be implemented at the county level. For political campaigns, CISA disseminated a cybersecurity best practices checklist to help candidates and their teams better secure their devices and systems.

On Election Day, DHS deployed field staff across the country to maintain situational awareness and connect election officials to appropriate incident response professionals, if needed. In many cases, these field staff were co-located with election officials in their own security operations centers. CISA also hosted the National Cybersecurity Situational Awareness Room, an on-line portal for State and local election officials and vendors that facilitates rapid sharing of information. It gives election officials virtual access to the 24/7 operational watch floor CISA. This set-up allowed DHS to monitor potential threats across multiple States at once and respond in a rapid fashion.

PRIORITIES FOR THE 2020 ELECTION CYCLE

For the 2020 elections, CISA has identified the following lines of effort to guide the Department's work:

- Protecting Election Infrastructure,
- Supporting Campaigns and Political Infrastructure,
- Raising Public Awareness and Building Resilience, and
- Efficiently Sharing Actionable Intelligence and Identifying Threats.

These priorities include broadening the reach and depth of information sharing and assistance that CISA is providing to State and local election officials, deepening our understanding of the elections risk environment, highlighting the need for regular and consistent resourcing of election infrastructure, extending the CISA suite of services for protecting networks to political campaigns and partisan organizations at the National level, and providing intelligence and threat reporting to the election

community. For more information on these priorities, please visit: *www.dhs.gov/cisa/protect2020*.

In addition, CISA is working toward improving the efficiency and effectiveness of election audits, incentivize the patching of election systems, and working with the National Institute of Standards and Technology (NIST) and the States to develop cybersecurity profiles utilizing the NIST Cybersecurity Framework for Improving Critical Infrastructure. The Department will continue to engage any political entity that wants our help. We are continuously working to mature our understanding of risks to this sector, improve our offerings, and to provide meaningful security guidance leveraging leading practices.

CISA has made tremendous strides on these efforts and goals and has been committed to working collaboratively with those on the front lines of administering our elections to secure election infrastructure from risks. In February, CISA officials provided updates to the Secretaries of State, State election directors, and members of the GCC and SCC on the full package of election security resources that are available from the Federal Government, along with a roadmap on how to improve coordination across these entities. DHS also worked with our intelligence community partners to provide a Classified 1-day read-in for these individuals regarding the current threats facing our election infrastructure.

In June, CISA hosted another "Tabletop the Vote" exercise with our Federal partners, State and local election officials, and private-sector vendors to review coordination protocols and incident response plans. The Tabletop covered a number of pre-, post-, and day-of election scenarios, including voter registration compromises, equipment issues, and misinformation distributed over news and social media. Participants included representatives from 47 States, thousands of local election officials, the District of Columbia, U.S. Virgin Islands, along with our Federal partners.

In July, DHS joined ODNI, DOJ, and DOD in briefing the full Congress on the Federal Government's coordinated approach to protecting the 2020 elections. DHS highlighted the increase in threat information that is now shared with State, local, territorial governments, the number of intrusion detection sensors, known as Albert sensors, deployed across the country, and the prioritization of intelligence sharing with State and local officials on cyber threats and foreign interference.

CISA, through the EI–ISAC, now provides threat alerts to all 50 States and more than 2,000 local and territorial election offices. CISA also provides weekly vulnerability scans for 37 States, 145 local partners, 1 territory, and 10 private-sector partners. In addition, all 50 States, 110 localities, and 2 territories now have intrusion detection sensors. These sensors are operated and monitored by EI–ISAC as part of the Multi-State Information Sharing and Analysis Center's (MS–ISAC) Albert intrusion detection system. DHS shares intelligence and other cyber threat information with EI–ISAC for use in Albert, which assists with identifying specific threats to election infrastructure networks. EI–ISAC has also deployed Albert sensors within election vendor environments, to protect their networks that host voter registration systems in 5 States.

CISA is also expanding our level of engagement with political organizations. We have worked in close coordination with both the Democratic National Committee (DNC) and the Republican National Committee (RNC) to share information and best practices. CISA has also engaged directly with Presidential and Congressional campaigns. These efforts have included a joint threat briefing with the FBI and ODNI for all Presidential campaigns registered with the FEC as well as engaging directly with campaigns to offer services and share information.

We will remain transparent as well as agile in combating and securing our physical and cyber infrastructure. It will take continual investment from all levels of government to ensure that election systems across the Nation are upgraded, patched, and better secured, with older more vulnerable systems retired. These efforts require a whole-of-Government approach.

Our voting infrastructure is diverse, subject to local control, and has many checks and balances. As the threat environment evolves, DHS will continue to work with Federal agencies, State and local partners, and private-sector entities to enhance our understanding of the threat; and to make essential physical and cybersecurity tools and resources available to the public and private sectors to increase security and resiliency.

Thank you for the opportunity to appear before the committee today, and I look forward to your questions.

Chairman THOMPSON. Thank you for your testimony.

I now recognize Mr. Sandvoss to summarize his statement for 5 minutes.

STATEMENT OF STEVEN S. SANDVOSS, EXECUTIVE DIRECTOR, ILLINOIS BOARD OF ELECTIONS

Mr. SANDVOSS. Thank you.

Good morning. My name is Steve Sandvoss and I am the executive director of the Illinois State Board of Elections. I would like to thank Chairman Thompson, Vice Chairwoman Underwood, and Congressman Casten for giving me this opportunity to address you.

As you are aware, in June 2016, the Illinois State Board of Elections was the victim of a cyber attack during which hackers gained unauthorized access into the voter registration database maintained by the SBE.

In response to this attack, measures were immediately undertaken to eliminate the vulnerability, assess the damage, and alert the victims and beef up our cyber defenses.

Following all of this, the SBE undertook an unprecedented effort to secure its voter registration database as well as other IT-related applications.

Such effort was assisted with a grant from the Election Assistance Commission that provided $380 million to the States to assist in their cybersecurity efforts.

Illinois' share was $13.2 million. Shortly after receiving this grant money, legislation was passed in Illinois that earmarked no less than half of the grant money to the Cyber Navigator Program to be created and administered by the State Board of Elections.

In order to receive any of the grant money, Illinois' election authorities who conduct the elections in Illinois were required to participate in the program.

The Cyber Navigator Program consists of three basic parts. The first part is the Illinois Century Network, which is a State-managed network delivering internet-type services to government agencies in Illinois.

The goal of the network is to provide the election authorities with a cleaner and safer internet. Having this network under the complete control of the SBE and the Department of Innovation and Technology ensures that voter registration and electronic canvassing data never actually flow over the internet. Additionally, this gives us the ability to provide security measures and intrusion monitoring.

The second part is the Cybersecurity Information-Sharing Program, which the SBE is overseeing in partnership with the Statewide Terrorism and Intelligence Center.

The program involves the research and gathering of information related to cyber attacks and cyber resiliency and sharing that information with all Federal, State, and local stakeholders.

Our goal is to consolidate numerous information sources and the feedback from the election authorities, distill it into the most valuable actionable information that is possible.

The third part are the cyber navigators themselves. Nine cyber navigators are currently on contract to assist the election authorities by performing on-site risk assessments and providing resources to ensure election security for 2020 and beyond.

The navigators will be offering additional services such as phishing assessments, penetration testing, and educational

trainings. They will also be performing assessments on physical security and best practices in securing voting equipment.

In additional to the Cyber Navigator Program, the SBE has worked in partnership with the Illinois National Guards' cybersecurity team to provide cybersecurity protection for both the State Board and the election authorities during the 2018 general election.

Members of the Guard were stationed in all regions of the State, at the SBE office, at the State-wide Terrorism Information Center, and at their own bases to be ready in the event of a cyber event.

We are planning on partnering with the Guard to provide cyber protection and incident response for the upcoming 2020 election.

Following the creation of the Cyber Navigator Program, the SBE released $2.9 million of the aforementioned grant funds to the participating election authorities to upgrade election-related computers systems and to address cyber vulnerabilities identified by the cyber navigators.

The funds can also be used to implement cybersecurity best practices for election systems and other activities designed to improve the security of the election systems.

In addition to the Cyber Navigator Program, the SBE took many steps to beef up its own internal cybersecurity and these steps are described in greater detail in my written statement.

Looking to the future, the SBE believes it is necessary to maintain the Cyber Navigator Program indefinitely and possibly expand it to address the continuing needs of the election authorities.

Cybersecurity is an on-going ever-escalating process that doesn't have an end date and, as such, there will be an on-going need for funds to maintain the program.

At present, the primary mission of the cyber navigators is to facilitate the Illinois Century Network connections between the SBE and the election authorities and to perform risk assessments of the IT systems of all the election authorities who are participating in the program to determine their adherence to the CIS controls.

The first phase of risk assessments is complete and the cyber navigators are currently reviewing each jurisdiction's vulnerabilities and are working with them to best utilize the security grant money to improve their cybersecurity posture.

In addition to the Cyber Navigator Program, the SBE is continually working on other ways to prepare for the upcoming election. We are assisting the election equipment management vendors to improve their security posture.

We have had discussions related to company ownership, personnel, cloud security, and processes for identifying cybersecurity risks, incident handling and recovery, testing, patching, and anomaly handling of hardware and software, and processes for handling the movement of data.

Our staff continues to participate in tabletop exercises that simulate cyber instances that could occur during an election. We are working with emergency management officials to coordinate preparedness for the upcoming election cycle.

Last, in conjunction with the Cyber Navigator Program and our Elections Operations Division, the SBE's public information officer

is developing a PR campaign to combat misinformation and disinformation particularly in social media.

I appreciate your time and consideration and will be happy to answer any questions you may have.

Thank you.

[The prepared statement of Mr. Sandvoss follows:]

PREPARED STATEMENT OF STEVEN S. SANDVOSS

OCTOBER 15, 2019

As the committee is aware, in June 2016 the Illinois State Board of Elections (SBE) was the victim of a cyber attack which at the time was of unknown origin. It has since been learned that the attack was perpetrated by Russian operatives who were seeking unauthorized access into the voter registration database maintained by the SBE. In response to this attack, measures were immediately undertaken to close the access point of the intrusion, assess the extent of the penetration, determine whether any data was manipulated or destroyed, and ascertain which voter records were improperly accessed, with the purpose of alerting said voters and giving guidance to assist them in protecting their sensitive information. It should be noted that an analysis of the breach did not reveal any evidence that specific voters were targeted or that the attack focused on any particular region or demographic. The SBE quickly alerted Federal law enforcement, and fully cooperated with their investigation. Following the initial steps described above, the SBE undertook an unprecedented effort to secure its voter registration database as well as other IT-related applications.

In March 2018, the EAC provided $380 million in grant money to the States to assist in their cybersecurity efforts. Illinois' share was $13.2 million, with a requirement that the State provide a 5 percent match; which amounted to $661,615. Shortly after receiving this grant money, legislation was passed in Illinois that earmarked no less than half of the grant money to a Cyber Navigator Program (CNP), to be created and administered by the SBE.

In order to receive any of the grant money, Illinois' Election Authorities (EAs) must agree to participate in the CNP. (The EAs consist of 101 county clerks, 1 county board of election commissioners, and 6 city boards of election commissioners, who are responsible for maintaining a list of registered voters within their jurisdiction, securing election voting and tabulating equipment and conducting the actual election on election day, as well as early and mail in voting.)

The CNP consists of 3 basic parts: (1) Requiring the EAs to adopt the Illinois Century Network (ICN) as their internet service provider for all traffic between their offices and the SBE, (2) Engaging in a Cyber Security Information Sharing Program with the EAs to share cybersecurity-related information, and (3) Creation of a team of "Cyber Navigators" to provide cyber assistance to the EAs.

ILLINOIS CENTURY NETWORK (ICN)

The ICN is a State-managed network delivering network and internet services to government agencies in Illinois. The goal of the ICN is to provide EAs with a cleaner and safer internet. The SBE Plan would bring all network traffic to and from the EAs to an internal "10 dot IP" network system and "whitelisting" IP addresses for access to the IVRS website. Isolating this network to one under the complete control of the SBE and Department of Innovation and Technology (DoIT) ensures that voter registration data and EA management operations never actually flow over the internet. Additionally, this provides us the ability to provide additional security measures and monitoring.

CYBERSECURITY INFORMATION-SHARING PROGRAM

In partnership with the Illinois State Police's division of State-wide Terrorism and Intelligence Center (STIC), the SBE is overseeing the Cyber Security Information Sharing Program, which involves researching and gathering of information related to pertinent cyber attacks and cyber resiliency and sharing that information with all Federal and State stakeholders. Our goal is to consolidate numerous information sources and, with feedback from local Election Authorities, distill it into the most valuable, actionable information possible.

CYBER NAVIGATORS

The Cyber Navigators are assisting the EAs by performing on-site risk assessments and providing resources to ensure Election Security for 2020 and beyond. Currently 9 Navigators are assigned in 4 regional zones in the State. (2 per zone, and 1 lead navigator). The Navigators will be offering additional services such as phishing assessments, penetration testing, and educational trainings. They will also be performing additional risk assessments on physical security and best practices in securing voting equipment.

In addition to the CNP, the SBE worked in partnership with the Illinois National Guard's cybersecurity team for coordination of a cyber defense system to provide cyber protection for both the SBE and the EAs prior to and on Election Day. Members of the Guard were stationed in all regions of the State, at the SBE, at STIC and their own bases to be ready in the event of a State-wide cyber event.

Following the creation of the CNP, the SBE released $2.9 million of the aforementioned grant funds to the participating EAs to make purchases to upgrade election-related computer systems and to address cyber vulnerabilities identified through the risk assessments performed by the Cyber Navigators and/or other assessments of existing election systems. Funds could also be used to implement cybersecurity best practices for election systems and other activities designed to improve the security of the election systems.

STEPS TAKEN TO IMPROVE THE SBE'S CYBER DEFENSES

In addition to the CNP, the SBE took the following steps to beef up its own cybersecurity.

- Hired 2 additional highly-experienced IT staff, including a Chief Information Security Officer (CISO) with over 20 years of Information Security experience.
- We have deployed advanced Next Generation Endpoint Security applications which protect agency systems from ransomware and other types of malware. This includes machine learning Endpoint Detection and Remediation (EDR) technologies to help with incident response, forensics, and remediation of security events.
- New agency perimeter firewalls have been installed which also includes network intrusion prevention systems. Web application firewalls were also deployed to protect our agency's public-facing applications.
- Secure Web Gateways have been deployed which provides category and reputation filtering to ensure agency internet traffic is protected from malicious sources.
- Our email security posture has increased significantly due to implementations of strict spam/phishing policies and creation of agency Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting & Conformance (DMARC) records.
- Data Loss Prevention (DLP) technologies have been deployed to protect against sensitive data exfiltration. We are also in the process of deploying full disk encryption solutions to our endpoints.
- We partner with the Illinois Department of Innovation and Technology to transfer network and system logs to their 24/7 Security Operations Center (SOC).
- We are running weekly internal vulnerability scans against all agency systems and websites. Illinois Department of Innovation and Technology is running weekly vulnerability scans against our public-facing websites. DoIT and DHS have also performed penetration tests and risk & vulnerability assessments.
- Future initiatives include implementations of additional email, DLP, log management and cybersecurity education technologies.

Looking to the future, the SBE believes it is necessary to maintain the Cyber Navigator Program indefinitely and possibly expand it to address the continuing needs of the EAs. Cybersecurity is an on-going, ever-escalating process that doesn't have an end date, and as such there will be an on-going need for funds to maintain the program. At present, the primary mission of the Cyber Navigators is to perform risk assessments of the IT systems of all the EAs who are participating in the CNP (all 108 EAs are participating in the CNP and have completed the first round of risk assessments). The EAs are in the process of evaluating the Assessments to determine what type of security enhancements are needed and are accessing the HAVA grant funds to cover the expenses. Some of the other steps that have been taken to enhance security leading up to next year's elections are as follows:

- Working with the election equipment and management vendors to improve their security posture. This involves a series of questions related to company ownership, personnel, cloud security, and processes for identifying cybersecurity risks,

incident handling and recovery, testing, patching and anomaly handling of hardware and software and process for handling the movement of data.
- Participating in Table-Top Exercises.
- Working with the Emergency Management officials to coordinate preparedness for the up-coming election cycle.
- Developing a PR campaign to combat misinformation/disinformation, particularly on social media. The SBE has produced videos to assist the election officials and voters on how to spot and report same as well as videos on how to maintain voting machine security and integrity.

Chairman THOMPSON. Thank you for your testimony.

I now recognize Ms. O'Connor to summarize her statement for 5 minutes.

STATEMENT OF ROBIN M. O'CONNOR, CLERK, LAKE COUNTY, ILLINOIS

Ms. O'CONNOR. Good morning. I am the proud Lake County clerk and leader of a stellar team within our office which provides multiple services to its citizens.

I do want to stop real quick and say thank you to the two gentlemen that have just spoken because we use their services and we are grateful for their offerings. They are steadfast with their constant support and we are very thankful in the counties.

OK. Continuing, I just want to talk a little bit about Lake County, Illinois. Lake County, Illinois protects the security and reliability of our election infrastructure.

We recognize the importance of using best practices, researching, and acquiring modern election systems architecture as well as collaborating with organizations dedicated to the guiding and providing us to the highest—Lake County has a population of 700,832, according to the U.S. Census Bureau Population Estimate Program 2018, and as of October 11, 2019, 458,586 registered voters.

There are 121 voting sites on the day of election and 18 early voting sites throughout the county. Lake County offers 3 voting options: Vote by mail, early voting, and Election Day.

Citizens may grace register to vote on early day—early voting up to and including Election Day. A snapshot of our election landscape is that we do have a network-connected system but it is not connected to the internet. It is our voter registration system.

We have an indirect connected system, which is our elected—election management system with e-pollbooks and we also have a nondigital elections component, which is our vote-by-mail process, which involves multi-steps.

There are parts which are digital such as on-line requests and signature verifications.

Lake County participates in the election—Illinois Election Cyber Navigation risk assessments, which was used to identify and assess impacts of vulnerabilities on our network and elections system. A common baseline risk assessment as well as examining the inherent complexities of network connectivity was conducted.

The results were as follows. We are proud to say that the Lake County IT department has already implemented many of the recommendations and we are working now on implementing the others recommended.

A common concern is the pairing of information between voter registration and election tabulation as well as connectivity. Both systems are separate and not connected.

Our voter registration system will soon be on the Illinois Century Network. ICN is a separate and private dedicated network for traffic between the Illinois State Board of Elections and our voting registration system. Our election tabulation system, again, is not connected to the internet.

Within our election systems and the mitigating risk policies we pride ourselves in being proactive and prepared for risks and threats.

I would like to talk a little bit about the management systems within our cybersecurity profile. At the county level, we are very fortunate because we have an IT security officer along with a robust IT department that has already implemented many of the cybersecurity measures protecting the county network and the IT systems, including our e-pollbooks, our voter registration, and our election tabulation systems.

At the State level, Lake County's Clerk's Office joins the Illinois Election Cyber Navigator Program and is working to implement recommendations from the risk assessment.

At the National level, the Lake County Clerk's Office joined the Election Infrastructure Information Sharing and Analyst Center and a multi-State Informational Sharing Analysis Center and we are receiving regular advice and recommendations from these organizations.

We are also adding an Albert sensor to our voter registration system which is a monitoring tool that looks for malicious traffic on our network and alerts for security operations center and it is a 24/7 analysis center that will investigate and provide resources to mitigate any issues on our network.

Finally, the Optical Scan Voting System that we use leaves a secure paper trail and minimizes the risk against outside interference as no electronic votes are ever cast.

All voting results can be accurately reproduced by reinserting the voter paper ballots through a ballot counter or a manual inspection.

The threats of election interference, we believe, as all of us who are here, is constant and requires proactive monitoring. To maintain always this election integrity, the Lake County Clerk and team values our citizens' confidence to keep their votes safe and secure.

[The prepared statement of Ms. O'Connor follows:]

PREPARED STATEMENT OF ROBIN M. O'CONNOR

OCT. 15, 2019

Lake County Illinois protects the security and reliability of our election infrastructure. We recognize the importance of using best practices researching and acquiring modern election systems architecture, as well as collaborating with organizations dedicated to guiding and providing us services of the highest merit.

Lake County has a population of 700,832 according to the U.S. Census Bureau Population Estimate Program 2018 and 458,586 registered voters as of October 11, 2019. There are 121 voting sites on the day of election and 18 early voting sites throughout the county. Lake County offers 3 voting options: Vote by mail, Early

Voting, and Election Day. Citizens may grace register to vote during Early Voting, up to and including Election Day.

Listed below is a snapshot of our election landscape:

1. Network connected systems and components (We are not connected to the internet): Voter Registration System
2. Indirectly connected systems: Election Management System, ePollbooks
3. Non-digital elections components: In this category our vote by mail process involves multi-steps. There are parts which are digital such as on-line requests and signature verifications.

Lake County participated in the Illinois Elections Cyber Navigators Risk Assessment which was used to identify and assess impacts of vulnerabilities on our network and election systems. A common baseline risk assessment as well as examining the inherent complexity of network connectivity was conducted. The results were as follows: The Lake County IT Department had already implemented some of the recommendations, and we are working on implementation of the others.

A common concern is the pairing of information between voter registration and the election tabulation, as well as connectivity. Both systems are separate and not connected. Our Voter Registration system will soon be on the Illinois Century Network (ICN), which is a separate and private dedicated network for traffic between the Illinois State Board of Elections and our Voter Registration system. Our Election Tabulation system is not connected to the internet.

Within our Election Systems and Mitigating Risk policies, we pride ourselves in being proactive and prepared for risks and threats. Listed below are management systems within our cybersecurity profile.

A. County Level.—Lake County has an IT Security Officer, along with a robust IT department that has already implemented cybersecurity measures protecting the County network and IT systems, including our ePollbook, voter registration, and election tabulation systems.

B. State Level.—The Lake County Clerk's Office joined the Illinois Elections Cyber Navigators program and is working to implement recommendations from the risk assessment

C. National Level.—The Lake County Clerk's Office joined the EI–ISAC (Election Infrastructure Information Sharing and Analysis Center) and MS–ISAC (Multi-State Information Sharing and Analysis Center) and receive regular advisories and recommendations from these organizations. We are also adding an Albert Sensor to our Voter Registration system, which is a monitoring tool that is looks for malicious traffic on our network and alerts the Center for Internet Security (CIS) Security Operations Center, a 24×7 analysis center that will investigate and provide resources to mitigate any issues on our network.

Finally, the optical scan voting system leaves a secure paper trail and minimizes the risk against outside interference as no electronic votes are ever cast. All voting results can be accurately reproduced by re-inserting the voted paper ballots through the ballot counter or manual inspection.

The threat of election interference is constant and requires vigilance to maintain election integrity. The Lake County Clerk and Team values our citizens' confidence to keep their votes safe and secure.

Chairman THOMPSON. Thank you very much.

I now recognize Ms. Howard to summarize her statement in 5 minutes.

STATEMENT OF ELIZABETH L. HOWARD, COUNSEL, DEMOCRACY PROGRAM, BRENNAN CENTER FOR JUSTICE

Ms. HOWARD. Thank you, Chairman Thompson, Vice Chairwoman Underwood, and Congressman Casten for the opportunity to testify today about the on-going efforts to secure election systems in Illinois and across the country.

Good morning. Election security has long been a priority for the Brennan Center starting in 2005 when we convened the Voting Systems Security Task Force to conduct the Nation's first systemic analysis of voting equipment vulnerabilities.

Our work continues today, and in my role as counsel for the Democracy Program, I have the opportunity to partner directly with State and local election officials as they work to implement impor-

tant election security measures, many of which we have supported for years.

As you have heard this morning, the election systems in Illinois and across the country were targeted in 2016, and according to our National security and intelligence officials will be targeted again in 2020.

In fact, the director of DHS's Cybersecurity and Infrastructure Security Agency—CISA—has stated the big game, we think, for adversaries is probably 2020.

While well-resourced hostile foreign nation-states may be a new addition to the list of actors who pose a threat to our election infrastructure, the tools and tactics they use are not. Cybersecurity professionals are very familiar with these threats including distributed denial-of-service attacks, hacking, and insider threats.

Considering this, it is no surprise that there is wide-spread agreement on the appropriate countermeasures and policies that are needed to ensure our election systems can withstand attack.

In short, we know what we need to do to harden our infrastructure but we are lacking in leadership and funding.

Illinois election officials are as acutely aware of the threats facing our election systems as anyone. Successful attacks on Illinois' voter registration database served as an unwelcome alarm to election officials everywhere and Illinois' efforts, including their successes and struggles, are instructive when analyzing the current National election security landscape.

In good news, election officials in Illinois and across the country have made significant progress in protecting our democracy since 2016.

In Illinois, these efforts have included identifying and addressing vulnerabilities in the voter registration database and launching the Cyber Navigator Program, which provides critical IT and cybersecurity support to local election officials.

This program is an important component of Illinois' efforts to secure its systems and serves as a model to other States.

Despite this progress, there is much to do in Illinois and across the country.

First, in Illinois, most of the voting equipment is antiquated and many of the machines do not use paper ballots. These machines need to be replaced immediately.

Next, Illinois should implement robust post-election audits that serve as a check on the election outcome and answer the question, "Did the reported winner really win the election?"

Next, many Illinois counties use electronic poll books. These are laptops or tablets that poll workers use instead of a paper list to look up voters at the polls.

There are no Federal or State security guidelines for this equipment. Illinois should consider expanding its current voting system security certification process to include electronic poll books and adopting common-sense contingency policies such as mandating paper back-up lists at the polls.

Of course, State and local election officials shouldn't be tasked with protecting our democracy alone. Congress has a very important role to play in the collective and comprehensive efforts to secure our infrastructure.

In my written testimony, I offer a number of recommendations for Congressional action. Among them, require voting system vendors to report cyber incidents.

Next, make the critical infrastructure designation permanent to ensure election security remains a priority at DHS and elections officials retain access to critical information and resources.

Next, Congress should pay its fair share of the on-going cost to protect our democracy and this funding should include responsible accountability measures such as those that were included in the budget bill that the House passed in June.

Thank you for your time. I look forward to your questions.

[The prepared statement of Ms. Howard follows:]

PREPARED STATEMENT OF ELIZABETH L. HOWARD

OCTOBER 15, 2019

Chairman Thompson, Ranking Member Rogers, and Members of the committee, thank you for the opportunity to speak about the critical issue of election security. The Brennan Center for Justice—a nonpartisan law and policy institute that focuses on democracy and justice—appreciates the opportunity to share with you our analysis of the important efforts to secure election systems in Illinois and across the country based on the results of our extensive studies and work to ensure our Nation's election systems are more secure and reliable across the country. We are deeply involved in the effort to ensure accurate and fair voting for all Americans.

For over a decade, I have worked on election administration issues. In my former position as Deputy Commissioner of Elections in Virginia, I coordinated various election security projects, including the decertification of all paperless voting machines in 2017. In my current role, I focus almost exclusively on election security. Representing the Brennan Center, I frequently partner with State and local election officials to assist with the implementation of important election security measures and serve on the Michigan Secretary of State's Election Security Commission and the Pennsylvania Secretary of State's Audit Working Group. I have also co-authored multiple reports on election security and remedial measures and policies that will better enable our election infrastructure to withstand attack.

Most recently, I co-authored Defending Elections, which demonstrates the need for additional election security resources across the country. This report includes detailed profiles of recent election security efforts and on-going needs in 6 States, including Illinois. We noted that as part of Russia's "sweeping and systemic" efforts to interfere with our elections in 2016, Russian operatives "compromised the computer network of the Illinois State Board of Elections . . . [,] then gained access to a database containing information on millions of registered Illinois voters, and extracted data related to thousands of U.S. voters before the malicious activity was identified."[1] And, although there is no panacea to counter such threats, Illinois has implemented a variety of election security measures which should help identify and patch or otherwise address cybersecurity vulnerabilities like those the Russians exploited in 2016.

Based on our extensive election security studies and partnerships with a diverse range of election officials, we believe that Illinois's successes and struggles in its on-going effort to secure the State's election infrastructure are instructive when analyzing the election security landscape across the country. In Illinois, and across the country, there has been much progress since 2016, but much work remains to be done.

I hope to convey 3 points in my testimony today:

(1) The risks facing our Nation's election infrastructure in 2020 require urgent action;

(2) Illinois has taken many important steps to improve election security, including implementation of a cyber navigator program, but there is more to do; and

(3) Congress has a critical leadership and partnership role to play in helping Illinois and other States ensure our elections are free, fair, and secure.

---

[1] Christopher R. Deluzio, Liz Howard, Paul Rosenzweig, David Salvo, and Rachael Dean Wilson, *Defending Elections,* Brennan Center for Justice, 2019, *https://www.brennancenter.org/sites/default/files/publications/2019__07__EACFunding%20Report__FINAL.pdf.*

A. THE RISKS FACING OUR ELECTION INFRASTRUCTURE MUST BE URGENTLY ADDRESSED.

Illinois was not the only State targeted by Russia in 2016. We now know that Russia likely targeted State and local election boards in all 50 States and used spear-phishing attacks to gain access to and infect computers of a voting technology company and 2 Florida counties.[2] We also know there is good reason to believe we face even more serious threats in 2020 and beyond. By 2020, the Russians will have had 4 years to leverage knowledge gained in 2016 to do more harm. Chris Krebs, head of the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security, has warned that the 2020 election is "the big game" for adversaries looking to attack American democracy.

In many ways, the major cybersecurity risks posed today by Russia and other hostile foreign nation-states are not new. They include hacking, e.g., SQL injections and ransomware attacks, distributed denial-of-service (DDoS) attacks and insider threats.[3] Like other Government officials responsible for protecting the integrity of IT systems and the information they maintain, election officials are struggling to manage these risks.[4]

Election officials hold a special place in our democracy. Not only are they responsible for protecting our election infrastructure, but also maintaining and bolstering confidence in the democratic process we use to decide who will serve important governmental roles at the Federal, State, and local level. Americans' faith in the integrity of this system is the foundation of our ability to self-govern and is in peril.[5]

Election officials should not be tasked with shouldering this responsibility alone. Under our Federal system of government, the risks facing individual election jurisdictions are a threat to every American who has confidence in our democracy. Successful attacks against our infrastructure in any county in any State can have a ripple effect that impacts the balance of power at the Federal level. While the decentralized nature of our electoral system is a strength in many ways, we are only as strong as our weakest link.

There is wide-spread agreement on many of the remedial measures and policies necessary to create a resilient election infrastructure. We urge Congress to take immediate steps to protect the votes cast by every American by passing common-sense legislation to ensure implementation of minimum election security standards across our Nation and by paying its fair share of the associated costs.

---

[2] *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1,* Senate Select Committee on Intelligence, 2019, *https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf* ("DHS assessed that the searches, done alphabetically, probably included all 50 States, and consisted of research on "general election-related web pages, voter ID information, election system software, and election service companies."); Miles Parks, "Florida Governor Says Russian Hackers Breached 2 Counties In 2016," *NPR,* May 14, 2019, *https://www.npr.org/2019/05/14/723215498/florida-governor-says-russian-hackers-breached-two-florida-counties-in-2016;* Sean Gallagher, "DHS, FBI say election systems in all 50 States were targeted in 2016," Ars Technica, April 10, 2019, *https://arstechnica.com/information-technology/2019/04/dhs-fbi-say-election-systems-in-50-states-were-targeted-in-2016/* ("The FBI and DHS assess that Russian government cyber actors probably conducted research and reconnaissance against all US States' election networks leading up to the 2016 Presidential elections."); Election Security Hearing, Before the Comm. on House Administration, 116th Cong. (2019) (Statement of Lawrence Norden).

[3] Meredith Berger et al., *The State and Local Election Cybersecurity Playbook,* Harvard Kennedy School and Defending Digital Democracy, 2018, *https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf.*

[4] See e.g., Kylie Bielby, "GAO: Federal Agencies Struggle to Manage Cybersecurity Risks," Homeland Security Today, July 26, 2019, *https://www.hstoday.us/exclude-from-homepage/gao-federal-agencies-struggle-to-manage-cybersecurity-risks/;* Alyza Sebenius and Kartikay Mehrotra, "States Struggle to Update Election Systems for 2020," *Bloomberg,* August 15 2019, *https://www.bloomberg.com/news/articles/2019-08-15/states-struggle-to-update-election-systems-ahead-of-2020;* Benjamin Wofford, "The hacking threat to the midterms is huge. And technology won't protect us," *Vox,* October 25, 2018, *https://www.vox.com/2018/10/25/18001684/2018-midterms-hacked-russia-election-security-voting;* Kate Rabinowitz, "Election Security a High Priority—Until It Comes to Paying for New Voting Machines," *ProPublica,* February 20, 2018, *https://www.propublica.org/article/election-security-a-high-priority-until-it-comes-to-paying-for-new-voting-machines.*

[5] Robert S. Mueller III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election,* U.S. Department of Justice, 2019, *https://www.justice.gov/storage/report.pdf* (characterizing the Russian government's interferences as a "sweeping and systematic" effort to undermine faith in our democracy).

B. ILLINOIS OFFICIALS HAVE IMPLEMENTED MANY IMPORTANT ELECTION SECURITY MEASURES AND POLICIES, INCLUDING A CYBER NAVIGATOR PROGRAM, BUT MUCH WORK REMAINS TO BE DONE AT THE FEDERAL AND STATE LEVEL TO ADDRESS SIGNIFICANT SECURITY GAPS.

In the wake of Russia's successful infiltration of Illinois' voter registration database in 2016, Illinois officials took prompt action to address identified vulnerabilities. Their work continues today. Illinois' on-going efforts to further strengthen their election infrastructure include welcoming public and private election security partners, such as the U.S. Department of Homeland Security (DHS), and taking advantage of a wide range of free resources available.

In addition, they are using the entirety of the State's 2018 Federal election security grant funds, approximately $14 million, for cybersecurity improvements. The hallmark of that effort is the State's cyber navigator program; the State plans to devote at least half of its Federal grant toward this program. While much progress has been made in Illinois, the 2018 grant funds were simply not enough to address all the State's critical election security needs. In fact, the Federal grant funds were similarly insufficient in every State leaving election officials across the country in a grim situation. They were forced to decide which critical election security projects to fund—and which not to. In Illinois, this meant no Federal funding was available for urgent needs such as replacing antiquated voting equipment.

Illinois' Cyber Navigator Program Addresses a Critical Election Security Need and Serves as a Model for Other States Across the Country.

In 2018, Illinois launched its cyber navigator program (CNP). As part of this program, cyber navigators with responsibility for geographic zones across the State work with local election officials to train relevant personnel and to lead risk assessments and evaluations, among other things. They fill a role akin in many ways to that of a chief information security officer for counties. Their assessment and evaluation efforts help officials identify vulnerabilities and determine where additional resources may be needed to shore up cyber defenses. The program's other principal components are infrastructure improvement, through the Illinois Century Network Expansion, and information sharing, through the Cybersecurity Information Sharing Program.[6]

This program addresses a critical problem facing many local election officials in Illinois and across the country: the lack of IT and cybersecurity support at the local level.[7] Without a State resource for cyber assistance, local election officials who do not have dedicated IT staff may be at greater risk of a successful cyber attack. These officials may not have sufficient resources to appropriately respond to identified cyber threats to local systems or equipment, such as those risks shared by the Elections Infrastructure Information Sharing and Analysis Center (EI–ISAC).

Federal, State, and local officials across the country and the Brennan Center support the wide-spread adoption of this program,[8] which has been identified as an important component of Illinois' comprehensive approach to securing the State's election infrastructure.

i. Most of Illinois' Voting Machines are Antiquated and Many Do Not Use Paper Ballots. They Must Be Replaced and Robust—Post-Audits Must Be Implemented.

Millions of Illinois voters will go to the polls to cast their ballot on Election Day 2020. They will encounter a variety of different voting machines at their polling place, from hand-marked paper ballot systems in some counties to antiquated Direct Recording Electronic (DRE) machines that produce a voter-verifiable paper audit trail (VVPAT) in others. As "the bulk of the voting machinery in Illinois is at least 15 years old,"[9] the on-going use of these machines expose voters to multiple security risks.

First, aging voting systems, in general, are a security risk and less reliable than voting equipment available today. Older systems are "more likely to fail and are increasingly difficult to maintain."[10] Many used in Illinois, such as the AccuVote TSX

---

[6] Deluzio et al., *Defending Elections.*

[7] Deluzio et al., *Defending Elections.*

[8] Deluzio et al., *Defending Elections; DHS Election Infrastructure Security Funding Consideration,* National Protection and Programs Directorate, Department of Homeland Security, June 13, 2018, *https://www.dhs.gov/sites/default/files/publications/Election%20Infrastructure%20-Security%20Funding%20Considerations%20Final.pdf.*

[9] Rick Pearson, "Illinois Pushes Millions Toward Securing Its Election Systems," *Government Technology,* August 5, 2019, *https://www.govtech.com/budget-finance/Illinois-Pushes-Millions-Toward-Securing-Its-Election-Systems.html.*

[10] Election Security Hearing, Before the Comm. on House Administration, 116th Cong. (2019) (Statement of Lawrence Norden); Josie Bahnke (Elections Director, Office of the Lieutenant

used in multiple Illinois counties, including DuPage County, are no longer manufactured so finding replacement parts will be increasingly difficult over time.[11] This problem exacerbates the reported system-specific security concerns with other older systems used in Illinois, such as the AutoMARK, including inconsistent vote tallying and reboot times of 15 to 20 minutes.[12] Moreover, these systems simply lack important security features expected of voting machines today, such as hardware access deterrents for ports.[13]

The continued use of antiquated equipment is a concern in many other States as well. We estimate at least some voters in as many as 38 States will cast their 2020 ballot on equipment that is more than 10 years old.[14] In November 2018, we estimate that 34 percent of all local election jurisdictions were using voting machines that were at least 10 years old as their primary polling place equipment (or as their primary tabulation equipment in all vote-by-mail jurisdictions).[15] Next, although VVPATs were "designed primarily for audit purposes," studies have found they have some significant shortcomings.[16] For example, one report examining VVPATs in Cuyahoga County, OH found almost 10 percent of the VVPAT tapes "were either destroyed, blank, illegible, missing, taped together or otherwise compromised," and 19 percent of the tapes indicated discrepancies with the reported counts.[17] Auditing VVPATs also takes more time than auditing paper ballots "due to the need to physically separate the ballots from the spool in the first count."[18] Finally, the results of least one study "suggest that people count optical scan ballots somewhat more accurately than VVPAT paper tapes."

Cybersecurity experts, including the National Academies of Sciences, Engineering, and Medicine, agree that DREs with VVPAT represent a security risk and elections should be conducted using human-readable paper ballots.[19] The U.S. House of Representatives recently indicated its support for replacement of all DREs by voting to

---

Governor, Alaska), Letter to Election Policy Work Group Members, July 18, 2018, *http://www.elections.alaska.gov/doc/info/180718%20EPWG%20Research.pdf* ("Today the DOE is at a critical juncture: Alaska's voting equipment and technology are outdated, difficult to repair and prone to failure.").

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

[12] Ruth Johnson (Oakland County clerk/register of deeds), Letter to Rosemary Rodriguez (chairperson, Election Assistance Commission), October 2, 2008, *https://www.eac.gov/assets/1/6/Oakland_County_Michigan_letter_regarding_ES_S_M_100_voting_machine_tabulators.pdf* (stating that 8 percent of M–100 fleet in Oakland County "reported inconsistent vote totals during their logic and accuracy testing"); "Election Systems and Software (ES&S) AutoMARK," Verified Voting, accessed May 4, 2019, *https://www.verifiedvoting.org/resources/voting-equipment/%20ess/automark/* (listing AutoMARK security concerns).

[13] Deluzio et al., *Defending Elections.*

[14] Norden and Cordova, "Voting Machine Security" (Forty-one States minus Alaska, California, and North Dakota).

[15] Ibid.

[16] Stephen N. Goggin et al., "Comparing the Auditability of Optical Scan, Voter Verified Paper Audit Trail (VVPAT) and Video (VVVAT) Ballot Systems," *USENIX The Advanced Computing Systems Association,* 2008, *https://www.usenix.org/legacy/events/evt08/tech/full_papers/goggin/goggin.pdf* ("While VVPAT and VVVAT systems are both designed primarily for audit purposes, the actual implementation of VVPAT auditing has not been free from problems. For example, the Election Science Institute (ESI) examined all aspects of election administration in Cuyahoga County, Ohio during the May 2006 primary election. The ESI report found that 10 percent of VVPAT spools were unreadable or missing, while 19 percent of the spools indicated discrepancies with the reported counts (ESI, 2006). Alternatives like VVVAT systems are still currently under development.")

[17] *DRE Analysis for May 2006 Primary: Cuyahoga County, Ohio*, Election Science Institute, August 2006, 6, *https://web.archive.org/web/20120330212509/http://votingindustry.com/TabulationVendors/1stTier/Diebold/esi_cuyahoga_final.pdf.*

[18] Stephen N. Goggin et al., "Comparing the Auditability of Optical Scan . . . "; see also Joseph Hall, "McCormack Hit Job Video on VVPAT," *Not Quite a Blog,* March, 23, 2019, *https://josephhall.org/nqb2/index.php/mccormack_vvpat_vid* ("Recounting VVPAT ballots cast during early voting on DREs in conjunction with the pilot program ran for the November 2002 election in Sacramento County, California proved even more labor-intensive. Sacramento County Registrar of Voters Jill LaVine, in Congressional testimony on July 7, 2004 reported "the recount of 114 VVPAT ballots took 127 hours, approximately 1 hour per ballot due to the complexity of the long ballot for that election.").

[19] *Securing the Vote,* The National Academies of Sciences, Engineering, and Medicine, 2018, *https://www.nap.edu/read/25120/chapter/1* ("Electronic voting systems that do not produce a human-readable paper ballot of record raise security and verifiability concerns.")

provide $600 million in election security funding to States and requiring those States that continue to use DREs to first use these funds to replace them.[20]

Illinois is 1 of only a small number of States that continue to use DREs with VVPATs as the primary voting system in 1 or more jurisdictions.[21] In 2020, Illinois may be 1 of as few as 7 States with counties that rely primarily on these machines.[22] The on-going use of DREs with VVPATs makes the current election infrastructure in Illinois slightly more secure than the infrastructure in the 8 States (Indiana, Kansas, Kentucky Louisiana, Mississippi, New Jersey, Tennessee, & Texas) we estimate will use paperless DREs in 2020.

DREs with VVPATs are more secure than paperless DREs because the VVPAT can be audited after the election. Unlike some States, Illinois does take advantage of this security feature by conducting an audit of these paper records to check and confirm electronic vote tallies. We estimate that Illinois will be 1 of only 24 States and the District of Columbia that will have voter verifiable paper records for all votes cast and require post-election audits of those paper records before certifying election results in 2020.[23]

Illinois relies on the traditional post-election audit method, in which the results from voting equipment in a specific percentage of precincts are reviewed. This method provides assurance that individual voting machines are correctly tabulating votes. Risk-limiting audits (RLAs) are a relatively new type of audit that provide assurance that election outcomes are correct by using statistics to analyze random samples of all votes cast. In 2020, RLAs will be required State-wide in Colorado and Rhode Island and may be conducted in lieu of traditional post-election audits at the county level in California, Ohio, and Washington.

The Brennan Center has long supported both a complete, Nation-wide transition to paper ballot voting machines and the implementation of risk limiting audits ("RLAs"), an efficient and effective check on election results, to ensure security and confidence in electoral results. Encouragingly, many Illinois counties and multiple States have made significant progress in replacing their aging and DRE voting systems in recent months and years. Cook County, Macoupin County, Arkansas, Georgia, Pennsylvania, and South Carolina have either completed the replacement of their DRE voting machines or are transitioning now.[24] In addition, election officials in at least 6 additional States are piloting risk-limiting audits, the "gold-standard" of post-election audits.[25]

ii. Multiple Illinois Counties Use Electronic Pollbooks. There Are No Federal or State Security Guidelines for Electronic Pollbooks. They Should Be Included in the Federal Certification Process and Illinois Should Consider Adopting a State Certification Process and Common-Sense Contingency Policies.

As of July 2019, 41 States, including Illinois, and DC use or authorize the use of electronic pollbooks in at least some polling places.[26] Electronic pollbooks (EPBs)

---

[20] Financial Services and General Government Appropriations Bill 2020 Report, House Committee on Appropriations, 2019, 3, 51–52, 112, *https://docs.house.gov/meetings/AP/AP00/20190611/109632/HMKP-116-AP00-20190611-SD003.pdf.*

[21] *Federal Funds for Election Security: Will They Cover the Costs of Voter Marked,* Brennan Center for Justice and Verified Voting, 2018, *https://www.brennancenter.org/our-work/research-reports/federal-funds-election-security-will-they-cover-costs-voter-marked-paper.*

[22] California has required replacement by 2020, Wyoming is replacing now, and North Carolina State law currently requires replacement by December 31, 2019. "Secretary of State Alex Padilla Sets Deadline for Counties to Retire Old Voting Machines and Modernize Election Infrastructure," California Secretary of State Press Office, February 27, 2019, *https://www.sos.ca.gov/administration/news-releases-and-advisories/2019/secretary-state-alex-padilla-sets-deadline-counties-retire-old-voting-machines-and-modernize-election-infrastructure;* "Funding Elections Technology," National Conference of State Legislatures, July 29, 2019, *http://www.ncsl.org/research/elections-and-campaigns/funding-election-technology.aspx;* "State Board to Consider Certification of Voting Systems," *North Carolina State Board of Elections,* July 23, 2019, *https://www.ncsbe.gov/Press-Releases?udt_2226_param_detail=767* ("Under current State law, DREs will be decertified in North Carolina on December 1, 2019, in favor of voting equipment that results in paper ballots for all voters. Proposed legislation pending in the N.C. General Assembly would delay the decertification date.").

[23] Norden and Cordova, "Voting Machine Security".

[24] Marley Arechiga, "Cook County Getting New Voting Machines For First Time In 13 Years," *WBEZ,* March 26, 2019, *https://www.wbez.org/shows/wbez-news/cook-county-getting-new-voting-machines-for-first-time-in-13-years/02665912-4298-4ac5-afe8-3b7bff079027;* Macoupin County Clerk's Office, "We are really excited that the County Board approved purchasing new voting machines at this week's meeting," Facebook, August 16 2019, *https://www.facebook.com/MacoupinCountyClerk.*

[25] Norden and Cordova, "Voting Machine Security".

[26] "Electronic Poll Books," National Conference of State Legislatures, July 15, 2019, *http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx;* Andrea Cordova,

are laptops or tablets that poll workers use instead of paper lists to look up voters. Most EPBs can communicate with other EPBs in the same polling location to share real-time voter check-in updates.[27] In addition to an expedited check-in procedure, shorter lines, lower staffing needs, and cost savings, one major benefit of EPBs is that they can make it easier to set up "vote centers" during early voting in some States, e.g., Illinois, or on Election Day in other States. Vote centers are "an alternative to traditional neighborhood-based precincts".[28] Anyone in a particular jurisdiction can vote there, regardless of where they live, possibly making voting more convenient, providing additional cost savings, and encouraging increased voter turnout.[29] If a county uses multiple vote centers, the electronic pollbooks can automatically sync during the day to ensure that once someone has voted in a particular location, they cannot vote in another location on the same day.

Despite these advantages, EPBs also have the potential to introduce cybersecurity risks. In a worst-case scenario, hackers could alter or delete voter data, even causing voters to appear as if they have voted when they have not. EPBs that require access to the internet can also pose problems in rural counties that lack reliable connectivity.[30] Unlike voting machines, there are currently no Illinois or National security standards for electronic pollbooks. Currently, the Help America Vote Act (HAVA), limits the Federal election administration agency's ability to create requirements for, test, and certify EPBs in the same way they do for voting machines. The Illinois State Board of Elections is subject to similar limitations and expanding the State voting equipment certification process to include EPBs would likely require legislative action.

In the absence of Federal certification standards, 12 States have developed a State-wide system of e-pollbook regulation and certification according to the National Conference of State Legislatures (NCSL) and some States have adopted common-sense contingency policies to ensure that voting can continue with minimal interruptions in the event of a successful EPB attack or failure.[31] In 2018, when 34 States used EPBs, only half required printed back-up paper pollbooks to be present in the polling place at the time voting began and, in 32 of the 34 States, we found no requirements in State law or regulation mandating a minimum number of provisional ballots.[32] Although some Illinois counties, such as Cook County,[33] voluntarily supply each polling place with a paper copy of the pollbook, or implement other common-sense contingency policies, Illinois should consider adopting an EPB certification process and appropriate EPB contingency measures.

The Brennan Center supports updating HAVA to allow the Election Assistance Commission (EAC) to create a certification program for all electronic pollbooks, as they do for voting systems, in order to encourage secure EPB systems Nation-wide. These additional responsibilities will require increased funding and staffing levels for the EAC to effectively test and certify EPBs.

C. A COMPREHENSIVE APPROACH TO ELECTION SECURITY REQUIRES CONGRESSIONAL LEADERSHIP AND PARTNERSHIP WITH FEDERAL, STATE, AND LOCAL ELECTION OFFICIALS.

While State and local election officials can take many important steps without Congressional action, these efforts will result in a patchwork of election infrastructure vulnerabilities across the country. Only Congress can establish minimum National election security standards to safeguard our election infrastructure and Americans' confidence in our electoral system. Congress should take several meaningful

---

"Want a Simple Way to Increase Election Security? Use Paper," *Brennan Center for Justice,* October 8, 2018, *https://www.brennancenter.org/blog/want-simple-way-increase-election-security-use-paper.*

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

[28] "Vote Centers," National Conference of State Legislatures, *http://www.ncsl.org/research/elections-and-campaigns/vote-centers.aspx.*

[29] Ibid.

[30] Andrea Cordova, "Want a Simple Way to Increase Election Security? Use Paper," *Brennan Center for Justice,* October 8, 2018, *https://www.brennancenter.org/blog/want-simple-way-increase-election-security-use-paper.*

[31] "Electronic Poll Books," National Conference of State Legislatures, July 15, 2019, *http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx.*

[32] Cordova, "Want a Simple Way to Increase Election Security? Use Paper".

[33] "Election Security," Cook County Clerk's Office, *https://www.cookcountyclerk.com/service/election-security.*

and simple steps to assist and support the on-going efforts of State and local election officials to ensure that our elections are free, fair, and secure.

i. Congress should require election system vendors to report cybersecurity incidents.

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

The Brennan Center recommends that Congress adopt a mandatory reporting system for all cybersecurity incidents for election vendors. While this may seem like a small step, it could have a large impact on the overall security position of election officials around the country. We know that the lack of transparency in vendor security is a significant vulnerability to election security. Private vendors were targeted in the 2016 election and are likely to be targeted again.[34] In fact, reporting requirements for cybersecurity incidents are a bare minimum, and we should be considering additional requirements such as vendor employee background checks and other lessons learned from similar critical infrastructure sectors.[35] The Brennan Center has documented some of the additional reasons for mandating such reporting in the 2010 report, Voting System Failures: A Database Solution.[36]

ii. Congress should make the critical infrastructure designation permanent.

In a decision subsequently affirmed by the Trump administration,[37] DHS Secretary Jeh Johnson designated election systems as "critical infrastructure" in January 2017.[38] This designation is given to "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, National economic security, National public health or safety, or any combination of those matters."[39] It is significant because it "enables DHS to prioritize cybersecurity and physical security assistance to election officials upon request."[40] Further, this designation emphasizes, both domestically and internationally, that election infrastructure possesses all the benefits and protections that the Nation has to offer.[41] "Finally, a designation makes it easier for the Federal Government to have full and frank discussions with key stakeholders regarding sensitive vulnerability information."[42]

In practice, this designation has resulted in many substantive partnerships and collaborations. For example, it "enabled DHS to lead the formation of an Election Infrastructure Subsector Government Coordinating Council (EIS GCC) and the pri-

---

[34] Lawrence Norden and Ian Vandewalker, *Securing Elections from Foreign Interference, Brennan Center for Justice,* 2017, *https://www.brennancenter.org/publication/securing-elections-foreign-interference.*

[35] Brian Calkin et al., *A Handbook for Elections Infrastructure Security,* Center for Internet Security, February 2018, *https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf.*

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

[37] *Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure,* Office of Inspector General, Department of Homeland Security, February 28, 2019, *https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-24-Feb19.pdf* ("Subsequently, Secretary John Kelly affirmed the designation during a Congressional hearing on June 6, 2017"); Chase Gunter, "DHS secretary reaffirms support for voting systems' critical infrastructure designation," GCN, June 7, 2017, *https://gcn.com/articles/2017/06/07/voting-systems-critical-infrastructure.aspx* (" 'I don't believe we should' back off on the critical infrastructure designation, [DHS Secretary John Kelly] told members of the Senate Homeland Security and Governmental Affairs Committee on June 6").

[38] "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," Office of the Press Secretary, U.S. Department of Homeland Security, January 6, 2017, *https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.*

[39] "Statement by Secretary Jeh Johnson," DHS.

[40] *Election Infrastructure Security Resource Guide,* Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, May 2019, *https://www.dhs.gov/sites/default/files/publications/19__0531__cisa__election-security-resources-guide-may-2019.pdf.*

[41] Ibid.

[42] "Statement by Secretary Jeh Johnson," DHS.

vate sector's Election Infrastructure Subsector Sector Coordinating Council (EISCC) to serve as collaborative forums where the Federal Government, State, and local government officials, and the private sector can establish mutually-recognized information sharing to prevent or mitigate the effects of incidents that undermine the integrity of or public confidence in the election system."[43]

Congress should make this designation permanent to guarantee States are provided with priority access to tools and resources available from DHS and greater access to information on cyber vulnerabilities on a voluntary basis.

iii. Congress should provide consistent and reliable funding for election security.

A lack of financial resources presents the most significant obstacle to election security improvements in local jurisdictions. Congress took an important first step in 2018 by allocating $380 million to States for election security activities, and there are promising signs of more funding coming in 2019. But these one-time investments are not enough to address the significant problems facing election systems or provide long-term stability for future election security planning. It is clear there is an on-going need for Federal funding to help protect our election infrastructure from foreign threats. As such, we recommend that the Federal Government increase its funding commitment to election security and invest in innovative approaches toward making elections more secure, accessible, and efficient.

Because the threats to election security evolve over time, effective election security requires an on-going commitment of resources, as opposed to a one-time expenditure. Companies in the private sector have departments and budgets dedicated to security generally, and often to cybersecurity specifically, precisely for this reason. Congress should provide a steady stream of funding for the periodic replacement of outdated voting systems, upgrading of databases and other election infrastructure, and the purchasing of on-going technical and security support for all these systems.

The Brennan Center has estimated the Nation-wide 5-year cost for 4 of the highest-priority election security projects to be approximately $2.2 billion.[44] This total includes estimated costs for: (1) Providing additional State and local election cybersecurity assistance, (2) upgrading or replacing State-wide voter registration systems, (3) replacing aging and paperless voting machines, and (4) implementing rigorous post-election audits.

CONCLUSION

Election officials in Illinois and across our Nation have made great progress since 2016 in securing our elections. But in an era when Americans' confidence in our democracy is at stake and hostile nation powers are likely to continue to see American election infrastructure as a target, we cannot rest on our laurels. As one election official noted in an interview with the Brennan Center, "we are trying to build the [protective] wall faster than our opponents are tearing it down." Doing so requires consistent, coordinated resources and leadership from all levels, including Congress, Federal agencies, the States, and local governments.

Chairman THOMPSON. Thank you very much.

I thank the witnesses for their testimony. I remind each Member that he or she will have 5 minutes to question the panel. I now recognize myself for questions.

Part of Ms. Howard's comments spoke to the varying degree of ability of certain communities to finance the machines necessary to conduct the elections.

Mr. Sandvoss, what has been your experience as to whether or not you have seen counties with the resources to do it on their own to buy additional equipment?

Mr. SANDVOSS. Well, my experience has been that, you know, the counties in Illinois vary along the largest and most—has the most resources and those who are small with very little.

So I think there is not a one-size-fits-all answer to that. But I do think that the voting machines, as it was pointed out being as

[43] *Election Infrastructure Security Resource Guide,* CISA.

[44] Lawrence Norden and Edgardo Cortés, "What Does Election Security Cost?," *Brennan Center for Justice,* August 15, 2019, *https://www.brennancenter.org/our-work/analysis-opinion/what-does-election-security-cost.*

antiquated as they are, are going to have to be replaced relatively soon if for no other reason, like any other piece of equipment after a while it starts to break down. It starts to—its life expectancy is coming to an end.

I think what we are facing right now is somewhat of a—you know, when I say we I mean the election authority community—is facing a little bit of a dilemma in the fact that voting machine manufacturers, while they can modify their systems—your existing systems, they can use patchwork and what not to, you know, keep them secure.

But we are all waiting for the voluntary voting system guidelines to be promulgated by the EAC. The voting system manufactures, my understanding is, are holding off on new development until they see those standards so they can manufacture the machines to those standards.

Once those standards an enacted and the machines are starting to be produced and, of course, they have to be tested, that is when, I think, the resources is going to be more of an issue and I think that is probably going to affect all the counties because replacing the voting machines is not going to be—not going to be cheap.

So once we are in a position to make a decision on purchasing those machines then I think big ask is going to take place.

Now, if our legislature can foot some of that bill, that is great. I don't—I mean, Illinois, like probably many other States, is not in great economic shape. Hopefully, we are getting better.

But even so, I don't know if that is a reliable funding source for the amount of money that it is going to take to replace all the voting machines.

Chairman THOMPSON. Well, one of the challenges we have as Members of Congress is we have been a partner with State and locals in some of that acquiring of new equipment.

But one of the problems we run into is we need to have standards, as you outline, in place so that vendors won't run out and just sell equipment just because it is new equipment. It needs to adhere to what we think the guidelines should be.

Mr. Masterson, one of the concerns that we heard early on is whether or not the Russians or some of these other bad actors conducted mischief in our 2016 elections.

What are you anticipating the potential for 2020 will be in the conduct of those elections?

Mr. MASTERSON. Yes, thank you, Mr. Chairman, and I appreciate the question. As, I think, Mr. Sandvoss mentioned and Ms. Howard, we at CISA and Director Krebs have been clear that we view the threat to election security as on-going and that 2020 is absolutely a target for nation-state actors and others to explore vulnerabilities not just in the systems but create disinformation campaigns in and around the elections process, which is why our focus isn't just on the cybersecurity side, although that is our primary focus in working with State and local official, but also empowering State and local officials to talk to their voters about the security measures they have taken, the resiliency of the process, that ability to audit the process and manage risks to the systems so that voters can proceed with confidence.

This is where our decentralized system is really effective because voters can engage directly with the folks that run the process in their community to ask the questions they have, to serve as poll workers, to watch pre-election testing of systems and really to understand the steps that are being taken to secure the process.

So from our perspective, the targeting of 2020 could come in the form of cyber operations or simply disinformation, or a mixture, and we really want to provide the tools and skills for the State and local officials to respond.

Chairman THOMPSON. Thank you. I have one additional question.

Ms. O'Connor, you were quite clear about your system here in Lake County and I compliment you for it.

Do you see the need either at the State or Federal level for additional resources that could be made available to you or what resources do you see as a local person you think the Federal or State government should provide to you as a local elected official?

Ms. O'CONNOR. I think the most—to be honest, they provide us advice and services. But I am—I come from a background of education so I am a strong researcher and I believe in education.

So I look to them for the newest methods, what is out there, how can they help us get there. So both State—the State—the Illinois State elections advisors have been so important to us.

Whenever we have a question we turn to them. We ask them. They give us advice and that allows us to research the best practice in the direction in which we are going.

Chairman THOMPSON. Thank you. I yield 5 minutes to the gentleman from Illinois, Mr. Casten.

Mr. CASTEN. Thank you so much, Chair Thompson. Thank you, Congresswoman Underwood, for allowing me to waive onto this committee and thank you for doing this in Illinois.

Given the hack that happened on our elections I think it is critical for us to let people know that we are actively working to fix this and thank you for having us out here.

It strikes me that there is 2 ways—you know, democracy depends on people trusting that their elections represent the will of the people and there is 2 ways that we can frustrate that.

One is we can go in and physically modify votes. The other way is we can do some sort of targeted suppression of votes. Certainly, in the pre-cyber era, I would submit to you that targeted suppression was much more prevalent.

It is more cost-effective, if you will, in terms of time and labor whether through poll taxes or literacy tests or polling place location.

My first question is for you, Mr. Masterson. In a cyber era, are you more concerned that hackers are going to come in and try to do more targeted suppression or are they—are you more concerned about physically altering individual votes?

Mr. MASTERSON. Yes, thank you for the question, Congressman.

From our perspective, as we analyze risk we certainly recognize that there is risk to the voting systems—those systems that both the voter interacts with and votes on and tabulates.

But at the same time, we haven't seen and there is no intelligence to suggest the actual targeting of those systems or attempts to change votes.

What we know is that adversaries are attempting to undermine our confidence in the democratic process including by creating doubt around a person's ability to participate, right.

So we worked throughout 2018 and continue to work now to share information with State and local officials so they can engage with their voters on simple messaging.

Understand, are you registered to vote before you head to the polls? Where are you registered? Where is your polling place? What is on your ballot? What can you expect to experience when you enter the voting booth and engaging directly with those who run the process?

Because the more voters know, the more attempts to discredit the process or to provide incorrect information to them, they have trusted sources of information at both the State and local level to combat that information, right—to go check the correct elections information and make sure that they are empowered to participate in the process.

So it is twofold, right. We worry about the infrastructure but we certainly worry—engage actively with State and local election officials on countering messaging around the elections process and, again, driving those voters to trusted sources of information—your State and local officials—to validate the information you need about that.

Mr. CASTEN. So I want to follow up with a second question but I just want to make sure I understand. So are you—do you think we are proportionately spending enough time on suppression as opposed to changing votes?

Mr. MASTERSON. I think proportionately we—so we think about it as a hybrid threat, right?

Mr. CASTEN. Sure.

Mr. MASTERSON. So there is concern about the infrastructure. Certainly, upgrading voting machines, having good consistent post-election audits, which counters that initial risk concern that you have laid out, is critically important to us and prioritized.

But equally important——

Mr. CASTEN. I am sorry. I just want to cut you off because I know that Madam Underwood momentarily——

Mr. MASTERSON. No, I apologize, sir.

Mr. CASTEN. Mr. Sandvoss, as you think about the attack on Illinois' voter files in the last election, I can see how that could have led to voter suppression, especially if I can target those votes and if I can go in and modify which, thankfully, we don't think happened.

I have a hard time seeing how that would change votes. Should I be—in light of that, is it reasonable for us to be concerned about attacks on voter suppression in Illinois versus changing votes, since that seemed to be the big attack in 2016?

Mr. SANDVOSS. Yes, I think from what happened in 2016, you know, there was no evidence that votes were changed, which was certainly fortunate.

Our registration system—I think there is some misunderstanding amongst the—you know, the general population as reflected by some of the questions that we get.

That is, is that the registration system is completely apart from the vote tabulation system. So even if the bad actors were to have manipulated the voter registration data, it wouldn't have impacted the actual counting of the votes.

So I think that point needed to be made.

Mr. CASTEN. But, potentially, it might have meant that when you showed up at your polling place you weren't a registered voter?

Mr. SANDVOSS. Well, here is the—one of the advantages of having a decentralized system is that each election authority has its own voter registration database, if you will, for their particular county.

So if voters came in, even if ours was compromised, they are going to be using theirs to determine whether or not a person is registered to vote and if they are where their—what precinct they would be voting in.

So unless a hacker were to get into their voter registration system and run amok, I don't think what happened to us would have impacted at the county level on Election Day.

Our system was hacked back in June and into July whereas the election was in November, so at least we had some time, you know, to——

Mr. CASTEN. I think—I think I am out of time so I will—I will thank you and I will yield back.

Chairman THOMPSON. Well, we are a little—you can have more time if you want——

[Laughter.]

Chairman THOMPSON [continuing]. Since we are in Illinois.

[Laughter.]

Chairman THOMPSON. Yes, we—OK.

Mr. SANDVOSS. I am sorry. Then the second—the other part of your question was voter suppression and being concerned about that or——

Mr. CASTEN. Yes. Really, just asking for your thoughts of whether the—whether the attack on—you know, at that higher level.

You know, there is the attack on the voting machine, which I think in public's mind we think about, and then there is the higher level attack on the actual election files.

In my small brain, if I am a hacker, that attack on the election files feels to me like something that could be a targeted suppression attempt. But doing that before an election I have a hard time seeing how that would have led to a changing vote.

So my question, really, is whether you—whether you would agree with the conclusion in my small head.

Mr. SANDVOSS. I would—yes, I would agree that it would not—the targeted suppression or the resulting targeted suppression from the attack on the database, in my opinion, would just be more toward the system as a whole.

In other words, if the voter registration system could be infiltrated by foreign actors, does that mean that the whole election could be manipulated by these same foreign actors.

I can see where that perception could be out there and, again, perception is reality. Even though we know that it couldn't have happened the way it was perceived that it could happen because,

again, there is no—there is no direct link between our voter registration system and the tabulation of votes.

But if people think that oh, elections is one big process inside a machine and that machine got hacked, they could say, heck, why should I bother voting because, you know, if it is so easy to hack then maybe my vote is not going to count, and that is where the danger is.

I think that is what the focus is going to be on in 2020 is, you know, through education, as Ms. O'Connor pointed out, educating the voters by saying that, hey, you might hear stories of targeted attacks on a voter registration system but that doesn't mean that your vote is not going to count.

Your vote is going to count, and that, I think, you know, needs to be, you know, impressed upon the general electorate so that they, you know, don't lose confidence in the integrity of the election. I think that is what our big concern is.

Mr. CASTEN. Thank you. I yield back.

Chairman THOMPSON. Thank you.

I now recognize the Vice Chair of the full committee, the gentlewoman from Illinois, for as much time as she deems necessary.

Ms. UNDERWOOD. Oh. Well, thank you, sir.

[Laughter.]

Ms. UNDERWOOD. I will ask the question. Thank you so much.

So I want to start with Ms. O'Connor. Thank you again for appearing on our panel today. I really appreciate your expertise and your work here in Lake County.

In your opinion, do you believe that voters and our election infrastructure are well-prepared here in Lake County ahead of 2020?

Ms. O'CONNOR. Absolutely. I truly believe that we are well-prepared. I am very confident. We want our voters to be confident in our system and I believe that they are.

Lake County moves forward not only using all of the resources that are provided. We research to find out other avenues that we can learn and excel in, but also we are proactive in educating our voters.

Our system, even within our office—when somebody calls our office, for example, they don't go into a waiting spot. They are—they are streamlined through the office where they are always—the call is always answered by a live person and their questions are answered.

This is very important to us because we believe that every question is important, and every time we answer somebody's question we believe that we have educated a family—a group—not just one.

There are many vectors of misinformation that are out there concerning elections. When I go speaking to different groups I continually get similar questions and my goal is to educate.

Our office's goal is to educate people with an understanding that what we are doing is correct and they should be confident that their vote is going to count. Every vote is going to count.

Ms. UNDERWOOD. Thank you.

So can you tell us a little bit about the Cyber Navigator Program, from your perspective, and specifically if we were to make improvements of—you know, if the Federal Government was going to scale up the program Nation-wide or authorize more money for

States like Illinois to deploy locally, what improvements would have that—has that program enabled Lake County to make locally and what improvements would you recommend to the program?

Ms. O'CONNOR. Absolutely. Again, like I said before, that we are very fortunate because our office is in the Lake County government building so we also have the technology advancements and support from the IT experts within the Lake County building.

But what we are receiving through our survey and how we are adapting to update our programs and move forward and advance is I consider stellar because I always like to look at our program as—this is a very general idea but I like to put it in very layman's terms because I know we always speak the language.

An election is often very language-motivated, but I like to say that often we are looked upon election as a castle and in our area we have the moat of our county building security.

But then we have the dragons of the State and the National—and also supporting us and giving us additional means and ways to protect our vote and our office.

Ms. UNDERWOOD. Thank you.

Mr. Sandvoss, what benefits does the Cyber Navigator Program offer the county election officials specifically in those counties where they have limited budgets at that local level, which forces them to make difficult resource allocation decisions?

Mr. SANDVOSS. I think the benefits that the Cyber Navigator Program or cyber navigators themselves provide to the election authorities is the introduction of a—like a whole new way of thinking, and even those that have IT departments, I think, you know, prior to the Navigator Program, even prior to 2016, were probably not focused as much on cybersecurity as they should have been, through no fault of their own.

I mean, cybersecurity, to us—you know, we had basic levels of security but, you know, when it comes to what was really needed there was nowhere near enough.

So I think what the navigators are doing is providing that education to the local jurisdictions and the ones that have more limited resources, which is to say they have no IT department at all, I think they are the ones that are providing probably the most benefit to, well, I will say the election authority community because, you know, the ones that are the most vulnerable it goes back to the chain being as strong as its weakest link.

I think what they are doing is they are introducing to the local election authorities, you know, basic concepts of security but then, you know, taking it through step by step by analyzing what is going to be needed in order to be as secure as they possibly can be.

I think that is probably the primary benefit that they provide.

Ms. UNDERWOOD. What proportion of the 108 jurisdictions—local election jurisdictions—would you say don't have that baseline of IT capacity or cybersecurity capacity?

Mr. SANDVOSS. To be quite honest, I can't give you a percentage because I just don't know. But, you know, anecdotally speaking from, you know, some of the hearings that we have conducted over the past couple of years, I think maybe two-thirds.

Ms. UNDERWOOD. Really?

Mr. SANDVOSS. Yes. When I say that, I mean don't have full-time IT divisions. They may have a—through their vendor they probably have a person on contract that can go in and perform IT services.

So I guess in that respect you could say everybody has at least one person that they can rely on. But if you are talking about an actual IT department with full-time employees, I mean, that would be my guess.

Ms. UNDERWOOD. OK.

Mr. SANDVOSS. I mean, I could certainly find out and get back to you on that.

Ms. UNDERWOOD. Sure.

Mr. Masterson, did you have anything to add on that in terms of proportions in our State or across the country?

Mr. MASTERSON. Yes. So I don't—again, anecdotally, I don't have specific numbers. But it is not uncommon for many counties' IT departments to have to support more than just the elections department if there is even a dedicated IT professional for the county.

In some counties across the country it is actually contracted out to private-sector vendors as well.

To your question, ma'am, if I may, on the cyber navigators, that hands-on keyboard both risk analysis and support is really critical.

We know the steps that need to be taken to harden our system's network segmentation two-factor authentication—all of those controls.

It is a question of how do we get that support, and I think what Illinois has done here is innovative and really helpful to those counties.

Ms. UNDERWOOD. Thank you.

Back to Mr. Sandvoss. Have there been any challenges deploying the cyber navigators to all 4 of the geographical election authorities in Illinois?

Mr. SANDVOSS. I think the biggest challenge was probably selecting the right people to be the navigators because at first you think of cyber and you think of—you know, you want people who are well-versed in IT and all the jargon and all the software and the hardware and what not, which, of course, is very important.

But since you are basically selling a concept to the election authorities, you needed to pick people that have not only the technical skills but the people skills—the ones that can go into a jurisdiction and not blind them with science but, rather, approach them in layman's terms, saying, OK, here is—first of all, I am here to help.

Second of all, you know, if you—you know, may I take a look at your systems. In other words, approach it from a standpoint of mutual respect as opposed to just giving orders from on high, and I think that was probably the biggest challenge.

But the second probably biggest challenge is, again, convincing all the jurisdictions that this is something that you have to take seriously and that even though cybersecurity up to now has been a remote or a foreign concept, it can't be thought of anymore like that because, again, you don't want to be that county on Election Day that the system collapses because you didn't do everything that you could have, and that was probably——

Chairman THOMPSON. Will the gentlelady yield?

Ms. UNDERWOOD. Yes, sir.

Chairman THOMPSON. One of the challenges we have is building the talent locally so those jurisdictions can do exactly what you are talking about. The challenge more so is the over-reliance on vendors versus the capacity.

So what happens is if Lake County didn't possess the resources and talent internally, they would have to rely on an outside vendor and that vendor may or may not be what you need.

But what we are trying—grappling with in Washington is how do we come up with some standards that we all can agree that every election system should have in order to be verifiable.

So the public policy issue for us is not to say Vendor X, Y, or Z, but we should say an election system in order to be verifiable must have 1, 2, 3, and that is the—that is where we are because we want to make sure that our system of electing our leaders is as honest and accurate as possible.

So to some degree, we put money out to States and locals as a carrot for coming and doing that. But, again, it is a partnership from the Federal, State, and local level and I think Ms. Howard's testimony—written testimony said it would cost us about $2 billion to replace the machines around. That is a lot of money. Illinois might be——

[Laughter.]

Chairman THOMPSON [continuing]. The exception. But I want you to kind of talk a little bit about how you came up with this $2 billion amount as a cost.

Ms. HOWARD. Yes, sir. Thank you, Mr. Chairman.

So our $2.2 billion estimate is the cost for 4 of the highest-priority election security measures that we have identified.

So that includes approximately $750 million to replace the antiquated and paper coding machines across the country and I think Mr. Dietrich at the Illinois State Board estimated that the cost to replace the antiquated equipment here in Illinois would be approximately $175 million.

Our $2.2 billion estimate also includes $100 million for audits over the next 5 years, approximately $500 million for voter registration infrastructure and cybersecurity improvements, and approximately $830 million to deploy, in essence, the Cyber Navigator Program that you have here in Illinois across the rest of the country.

Chairman THOMPSON. Thank you. I yield back.

Ms. UNDERWOOD. Thank you.

So my next question is for Ms. Howard. In the report that you co-authored you mentioned 2 underfunded election security projects in Illinois—the adoption of countermeasures for security vulnerability identified through the risk and vulnerability assessments and legacy voter and system replacement, which we talked about a few times here.

Can you expand on your research and do you have any specific recommendations as to how Illinois can address those needs?

Ms. HOWARD. I think, you know, as you mentioned, in Illinois the 2 unfunded election security projects that we identified in working with State and local election officials were, you know, deploying ad-

ditional counter-measures based on the findings of the local cyber navigators and to replace the legacy voting equipment.

So these priorities are exceptionally important for a lot of reasons and I think that, you know, you can address these in Illinois promptly, and in Illinois you have a decentralized system.

So every county is going to be able to decide when and what type of equipment they are going to purchase when they purchase new equipment and I understand that Cook County has recently moved forward with purchasing new equipment and Macoupin County has recently decided to move forward and purchase new equipment. So it is moving forward on a county-by-county basis.

Ms. UNDERWOOD. I see. Thank you.

So the Senate Intelligence Committee has noted that election systems that use these optical scanners to review paper ballots are the least vulnerable to cyber attacks, and I understand from Ms. O'Connor that that is what Lake County uses as well.

What vulnerabilities are associated with the use of electronic voting systems without the optical scanners and then how many States would you say Nation-wide are using paperless voting machines in 2020?

Ms. HOWARD. Thank you for your question.

As you have heard today, the auditability of a system is an integral component of making it a resilient system and auditability is just a critical step that all of our systems need to have.

When you use a direct recording electronic, a DRE—a paperless DRE system, you cannot conduct a robust post-election audit on that. So that is the concern that we are looking at.

Right now we estimate that in 2020 there will be 8 States that continue to use paperless voting equipment as their primary voting equipment in one or more counties and those 8 States are Indiana, Kansas, Kentucky, Louisiana, Mississippi, New Jersey, Tennessee, and Texas.

Ms. UNDERWOOD. Thank you.

How much funding would the Federal Government need for the full—that is the $750 million you said—and then of that $750 million how much did Illinois get to make these changes that you recommended?

Ms. HOWARD. So it is going to depend upon the vehicle that Congress uses to deploy these funds. So if it is based on whether or not the State needs to replace antiquated or is using equipment that is more than 10 years old, the total number is going to be a little bit different than if you used it through the current HAVA formula.

Ms. UNDERWOOD. I see. But it would need to be robust by then?

Ms. HOWARD. Yes.

Ms. UNDERWOOD. OK. Thank you.

So in preparation for this hearing I asked our constituents in the Illinois 14th about their thoughts on what we should be doing to secure our elections.

Within a matter of days, my office received 258 responses from people all over the 14th District. Election security is, clearly, at the forefront of people's minds here in district.

So I want to use the remainder of my time to bring forward some of those constituent questions. The first is from Ryan from Oswego, Illinois, and this is to Mr. Masterson and Mr. Sandvoss.

What steps are being taken to prevent this structured query language, or SQL, injection attack from occurring again? For the folks here, it was that type of attack that the Russian operatives used in 2016 to penetrate the State Board of Elections.

Mr. SANDVOSS. Well, I would—the step that we took is we closed the portal in which the SQL injection entered into our system.

It was a design flaw in the paperless on-line voter registration application system where the voter is—checks to see what their registration status is and there was a window there that should have had a restriction on the number of characters, and for whatever reason that feature wasn't on there.

Ms. UNDERWOOD. I see.

Mr. SANDVOSS. So we discovered what had happened pretty quickly and immediately corrected it. I would say, going forward, we have—we conduct risk assessments in penetration testing, which basically bombards our system with different types of malware, including SQL, just to see if there is any other open windows, so to speak, and so far we haven't found any.

So that is—I mean, you still check on a regular basis just to make sure. But that is—that is the steps we have taken.

Ms. UNDERWOOD. That is great.

Then Peter from Island Lake had a related question—should there be a hard-copy back-up for all Illinois elections in case of hacking and do we have an emergency response team in our State in case hacking is detected?

Mr. SANDVOSS. As far as the second part of the question, I would say we do have an emergency response team. I think it is a cooperation effort between the State Board of Elections, the Statewide Terrorism Information Center. We are working with the DHS as well as the National Guard.

So I think that we would have personnel that are ready to go on a moment's notice responding to a cyber incident before, during, and right after the election.

Ms. UNDERWOOD. Thank you.

Mr. SANDVOSS. So—I am sorry, what was the first part of the question?

Ms. UNDERWOOD. The hard-copy back-up of all elections.

Mr. SANDVOSS. Yes. I mean, a hard copy could be produced. It probably would be a good idea to have.

I guess the only problem with that is that now that we have grace period registration, same-day registration, that list would constantly be changing.

So at what point do you print the list or have the back-up? Because every day it could be different. Somebody could be off the rolls, on the rolls, and so you would have a lot of supplemental lists.

But I guess, in general, if there was a major hacking incident and the whole registration—the electronic part of it went down, having a paper back-up would be—would be useful.

Ms. UNDERWOOD. OK.

Mr. Masterson.

Mr. MASTERSON. Yes, just very quickly, ma'am. Thank you for the question.

Certainly, taking regular backups both on-line and off-line, understanding where those dependencies are is absolutely critical, and then having an incident response plan and exercising that plan.

So implementing those back-ups and knowing they are going to work when you need them is something we recommend and work with through tabletop exercises and other work with the State and local so that there is that plan in place and they can actively respond if something occurs to whether the voter registration list or other systems.

Ms. UNDERWOOD. Did you want to mention the EIISAC that could be maybe not the emergency response but certainly does help——

Mr. MASTERSON. Yes——

Ms. UNDERWOOD [continuing]. States and municipalities——

Mr. MASTERSON. Absolutely. So the EIISAC provides both information sharing and response. DHS CISA provides incident responders both remotely but also that can deploy and get operations back up and running to mitigate the impacts of a cyber attack. So we have any number of resources that we could bring to bear, and thank you for asking that.

Ms. UNDERWOOD. Sure. OK.

So Paul from Naperville wants to know, is there any way to know if my personal voting information has been compromised?

Mr. SANDVOSS. Assuming he is referring to the 2016 database breach, he would have been notified.

Ms. UNDERWOOD. OK.

Mr. SANDVOSS. If there was enough information that we could determine a specific voter, we were required by law to notify that voter and we did, and then we provided the voters who were affected with options or resources that they could use to determine whether or not the information was improperly used.

To my knowledge, I don't think that anybody suffered any type of loss as a result of—like, economic loss as a result of the hack or if they did they haven't come forward to us and reported it.

Ms. UNDERWOOD. So we haven't spent a lot of time here today talking about social media companies, the misinformation, disinformation. Congressman Casten raised it during his line of questioning earlier and I think that that is an important piece of this.

So I want to know from Ms. O'Connor do you all have any kind of capacity to do anything on-line to combat that misinformation or are you more relying on people if they have a question to proactively reach out to your office?

Ms. O'CONNOR. We do that—we do it. We are very involved in social media from our office. So we are always delivering, you know, correct information, you know, on our Facebook page and all that—the modern social media aspects that today's world has.

So, again, our office believes in this educating and if somebody asks a question on our Facebook page we will correct them. You know, so in that respect, yes, we are involved in social media.

Ms. UNDERWOOD. OK.

Ms. O'CONNOR. Yes, we are active in correcting and educating our constituents.

Ms. UNDERWOOD. Awesome. Do you all have recommendations for how people should flag misinformation or disinformation? Do you all receive it at the State Board of Elections or is CISA doing anything in that respect as well?

Mr. MASTERSON. So I can start. So yes, absolutely. We have direct lines of contact with all the major social media companies.

Throughout 2018, State election officials and local election officials reported activity that we were able to pass on not just to the platform that had the activity but to all the platforms so they could look to see if it was cross-platform activity.

We don't recommend any actions to take on the activity but we are able to pass it on and say, here is activity that has been reported to us. Here is the contact for the State or local election official reporting it.

I will say when it comes to responding to disinformation around the elections process of misleading on where to vote, when to vote, things like that, the social media companies took a very aggressive posture and have published policies about takedown processes regarding that kind of activity and we are able to push that to them.

Ms. UNDERWOOD. So Christina from Batavia wants to know, is there anything that citizens should watch for on social media that might be signs of intrusion or election interference?

Mr. SANDVOSS. Well, I guess it depends on how knowledgeable a given person is with respect to voting procedure. I mean, if—obviously, if you see something that says oh, Election Day has been canceled—voting will start, you know, a week from today or something like that, you know, if it raises a red flag, if it doesn't make sense, if it just seems not right, we are going to encourage people to report it. You know, if you see something say something. So it is those types of things that——

Ms. UNDERWOOD. Report it to you or report it to the platform?

Mr. SANDVOSS. Well, right now I think we are trying to decide how we are going to do that.

Ms. UNDERWOOD. I see.

Mr. SANDVOSS. Yes. We haven't solidified that yet. But I think the idea will be to communicate it probably to us and then we would distribute it to our partners and then it would some—you know, it would eventually make its way to these—whatever social media company it originated from to get it corrected.

So it is examples like that that we are going to try to, you know, to put out and are included in our, you know, PR campaign, if you will, you know, trusted source and, first of all, you know, trusted source—specific county clerk or the Board of Election Commissioners or the State Board of Elections.

So if you see something that doesn't, you know, purport to be from an official Government agency, question it and then, second, like I said, if it just doesn't smell right, you know, say something.

Even if you are wrong doesn't matter. You know, at least it is communicated and you are being vigilant. So we are going to—we will, you know, put out basic things like, you know, no, there is no internet voting.

So any website that purports to say, you know, vote over the internet, ignore it. It is wrong.

Ms. UNDERWOOD. Right.

Mr. SANDVOSS. You know, voting—you know, Election Day is, you know, November 6 or 5 or whatever day it is. You know, if you get a post that says Election Day has been postponed or, you know, Democrats vote on Tuesday and Republicans vote on Wednesday—things that just don't make sense, you know, please, you know, alert us to that and we can get that—we can get that taken care of.

Ms. UNDERWOOD. One of the students who is here had a question. It is J.R.—I don't know which one is J.R. Do you think that it is going to be a recurring problem of other countries interfering with United States Presidential elections as well as distributing propaganda on social media?

So we talked about how the cybersecurity piece we knew was going to be a recurring threat. But just to put a pin in it, do we think that this social media disinformation will also be a recurring theme for 2020 and beyond?

Mr. MASTERSON. Yes, absolutely. I mean, the attempts by adversaries to undermine confidence in our democratic institutions as a whole is an on-going and robust effort from a variety of adversaries.

So absolutely. We view 2020 as a prime target for that as well as other democratic institutions.

Ms. UNDERWOOD. Awesome. Well, I can't stress enough the importance of today's hearing and the educational benefit that it has provided to our committee and to the public.

As I said before, the election is around the corner, less than 6 months until the primary, and we have to seize on every opportunity to have meaningful conversations like this one.

Thank you, and I yield back.

Chairman THOMPSON. Thank you.

Mr. Casten has some additional questions.

Mr. CASTEN. Thank you.

The—so I want to follow on—pick up some of what I was asking before about the sort-of targeted suppression angle in addition to changing votes and I—I am not a IT expert by any stretch but I spent 16 years as the CEO of energy companies, first as a manufacturer of power generation equipment and then running utilities.

A part of our job was to figure out where the vulnerabilities were and close those doors, which is why—which is why I am, at least, personally hypersensitive to this issue.

There is one question of how you suppress votes. There is a separate question of how you target them. Having recently won my first-ever election, it struck me that the—a campaign office is a beautiful place to hack into that election system because you have got tens, hundreds, in Congresswoman Underwood's case and I, thousands of volunteers showing up in uncontrolled offices, papers all over the place, and doing something that by its nature is partisan, which means that sometimes getting National support is a little less than it should be.

Mr. Masterson or Ms. Howard, I wonder if you have thoughts on are we doing enough to secure the voter data on the campaign side

of what we do up on this side of the dais and, if not, what can we do more at a National level so that all that doesn't fall on campaigns or political parties to provide that protection? Because if I have that data I know exactly who to target.

Ms. HOWARD. I think Matt may be better to answer this because he—they work directly with campaigns and candidates.

Mr. CASTEN. OK.

Mr. MASTERSON. I appreciate the question, and we have been working with DNC and RNC in campaign committees as well as individual campaigns in both outreach with information sharing and the same support and services that we offer for free to State and local election officials are available to these campaigns, all with the goal of managing the rest of their infrastructure.

Specifically to voter data, a big part of the voter registration data is publicly available already, right. That is how campaigns get a lot of it. So it is understanding what additional data is there and how they can secure that data, working with vendors primarily, right.

So understanding the third-party risk, and then managing that human element is a huge part of managing campaign risk, right.

So you hit on it directly, Congressman, and that is that there is volunteers, pop-up employment opportunities throughout campaigns and so how do we build-up resilience in the people engaged in the campaign work through phishing campaign assessments, through targeted education campaigns. So we have worked very closely with the campaigns to try to raise that awareness.

We created a very simple election campaign security checklist that we worked with both DNC and RNC on and then pushed it out through their channels in order to just give the simple steps that whether you are a volunteer or the candidate yourself that you can take to manage the risk to your systems, personal devices and otherwise, to protect that data that you have whether it is voter data or just important campaign communications, right.

Mr. CASTEN. My sense is that that—my experience is that that was more an opt-in than an opt-out program, right, because you still have volunteers showing up with their own computers. You know, by design you are not using a Government computer that has been Government-secured for those.

You know, I think, you know, we certainly tried to do a lot on our end but, man, it felt like a hole to me. Is there a way to make that an opt-out program?

Mr. MASTERSON. So all of our services, all of our support are voluntary and so it is really a question of, how we can best engage with the campaigns to either get that information out or the support and services?

I will say that both the RNC and DNC, in working with them, have taken a lot of actions, a lot of engagement opportunities with their campaigns and others to build that awareness.

But it is a big challenge for many campaigns and, candidly, it starts with the candidate. When the candidate prioritizes cybersecurity in a campaign, the rest of the campaign prioritizes.

Mr. CASTEN. Ms. Howard.

Ms. HOWARD. Thank you. I would just add that the Federal Election Commission has been working with nonprofit organizations on options to provide cyber assistance to campaigns free of charge.

But, as you know, there is no quorum currently at the FEC so this is a problem.

Mr. CASTEN. Mm-hmm. So I want to touch on something that Congresswoman Underwood raised. The social media question, to me, is less about does somebody say that is false on social media, do they get bad information as much as does that information then atomize and go out?

So the—you know, what Russia did in the United States in 2016 was not substantively different. It is different by scale but wasn't substantively different from the way they did it in Estonia or in Georgia or even in their own country.

They create social media campaigns to establish that voters cannot trust their institutions and at that point the institutions are weakened because that is Russia's national agenda.

That is a hard genie to put back in the bottle in a very atomized media environment. But my question really for all of you is that we, as public officials, have a duty to make sure that our election systems are as robust and protected as possible.

We also have the bully pulpit, and if we—if we exaggerate this fear beyond a reasonable level, the risk is that people might say, well, look, you know, all of these Members of Congress what they are saying, you can't trust your election system, in which case the Russians have exactly what they want.

So you 4 who are experts in this, how would you like to see us as public officials talking about this issue in a way that is both responsible and focused on closing barn doors where they are open but doesn't in any way over-stoke the fear beyond what is reasonable?

Mr. SANDVOSS. Well, I will speak from my experience and, granted, this isn't coming from, you know, elected Members of Congress. This is coming more from the DHS.

But it is certainly appreciated as the communication of the threats that are out there so that we know what is to expect and then we, at the State level, can decide how we want to present that to our general public.

I agree, it is a fine line between being—you want to project an aura of confidence because—I get this question all the time, how confident are you in the security of the elections leading up to 2020?

I want to say that I am confident but I don't want to sound like I am overconfident because then—you know, I know that systems can get hacked into and I know that, you know, foreign actors can engage in misinformation that could be successful.

So to make a prediction that I know might not come true would be kind-of silly. By the same token, you want to project an attitude of confidence that at least, hey, we are doing everything we can to, you know, make the elections secure.

We think they will be secure. Your vote—we think it will count. I mean, not say think. We know it will count. Then, you know, just—you know, put people's minds at ease.

I mean, obviously, there is a threat. Everybody knows it. But try to put their minds at ease and, to me, it is no different than anything else one might do.

I mean, are you going to not go outside because you risk getting hit by a car or not fly because you think your plane is going to down?

People still live their lives and I think, you know, with voting it should be the same way that, yes, there is risks. Yes, something could happen.

It might result in a line and it might result in me having to cast a provisional ballot. But, ultimately, at the end of the day, my vote is going to count and I think that is the message we want to send.

Ms. O'CONNOR. I am just going to comment that we work really hard to develop a trust and that, to us, is significant. We inform our citizens when we go to conferences, when we go to workshops.

For example, the Illinois workshop for clerks we talked about at that workshop how we have a back-up plan. We talk about our assessments. We are educated on what we should do next.

But we also look at each other as a community of Illinois clerks or as a community of clerks Nation-wide, and I think that is important because we communicate our ideas.

For example, I will get calls from other clerks saying, you know, what are you doing for this—how are you sending that information—can you share it.

We are a community of clerks within the State of Illinois and I think that is very crucial because as we move forward in that, you are not only developing trust but you are also developing a huge network of support.

Ms. HOWARD. I would say that I agree that there are 2 distinct issues, right—attacks on our infrastructure versus disinformation and trying to suppress the vote. But I think that they are linked.

Part of what they do with their disinformation campaigns is to exploit the concerns that people have about our infrastructure and investing in our infrastructure to strengthen it and to inform the public, right.

But it can withstand attack is a very important piece of this and kind-of, you know, looking back. I think Illinois election officials have really been pioneers in discussing this issue in an open and frank manner and have really helped election officials across the country figure out what is going to work for them as far as, right, striking the right balance between being honest and forthcoming about what is going on, right, but still ensuring that people have confidence in their voting system.

Mr. MASTERSON. Just quickly, sir—I really appreciate your question. I think Americans—most Americans have been impacted by cyber incidents, right. So they recognize there are vulnerabilities in systems.

So having an open discussion about what vulnerabilities may exist, what steps the folks at this table are taking to address those vulnerabilities, what more could be done to improve the resilience of the process.

All of us should be engaging voters in those conversations so that they can understand. They are not—they are not going to believe if you say everything is fine because they have been impacted by incidents like that.

Then talking very candidly between Members of Congress and election officials—it is why I appreciate this hearing so much—so

that you can understand how they view the risks, how they talk about the challenges to the process and have built resilience, whether it is through auditing, through a provisional balloting process, and then engaging your constituents in what steps they can take.

Because it really is—as the Chairman said, it is a whole-of-government but it is a whole-of-Nation response and they—voters have the ability to ensure that their registration information is up-to-date and correct, that they know their polling place, what is going to be on the ballot—that they know they have a right to a provisional ballot such that if there is a problem at the polls they can still cast a vote and know and actually get the information from the State that their vote was counted as cast is critically important.

So I think an honest discussion about both the risks in the process, the vulnerabilities, but also the steps that have been taken and continue to need to be taken is really critical as we move forward.

Mr. CASTEN. Thank you. I yield back.

Chairman THOMPSON. Thank you. Yield additional questions to the gentlelady from Illinois.

Ms. UNDERWOOD. Yes. Great conversation. Thank you, Mr. Chairman.

It dawned on me that we did not talk about the results—the notification of the findings and making sure that there is a trust that those findings are correct.

Have you all identified any vulnerabilities within the State of Illinois' reporting systems or across the country, and if anybody could just characterize any steps that are taken to ensure that not just the votes are counted but as they are reported on Election Night the American public can trust those findings to be correct.

Ms. HOWARD. Thank you for the question.

I think your question goes to the—again, the auditability of the system. So right now we have 24 States, we estimate, in 2020 that will conduct post-election audits before certification using the paper ballots, right.

Again, to go back to your question of confirming that the winner actually did win the election. We think, while Illinois conducts what is called a traditional post-election audit where they look at a predetermined percentage of votes cast in particular polling locations, that there is a better method.

We think the risk-limiting audit would answer the questions that you have and that lots of other voters have, and that it is something that, you know, we hope to work with Illinois election officials on in the future.

Ms. UNDERWOOD. Thank you. Thank you all.

Yield back, Mr. Chairman.

Chairman THOMPSON. Thank you.

Well, let me thank our witnesses for their valuable testimony and the Members for their questions.

The Members of the committee may have additional questions for the witnesses and we ask that you respond expeditiously in writing to those questions.

But I can say from the witness testimony so far as Illinois is concerned and Lake County specifically you are headed absolutely in the right direction.

From our vantage point in Washington, you are doing exactly the kind of work that we envision the rest of the country should do and we encourage that.

We go back to Washington this afternoon with a new sense of hope that the investment we put in under the HAVA last payment we can, hopefully, get new money into the system to give greater capacity to the State and locals toward improving their system of elections.

So hearing no further business, the committee stands adjourned.

[Whereupon, at 11:38 a.m., the committee was adjourned.]