S. HRG. 115–92

RUSSIAN INTERFERENCE IN THE 2016 U.S. ELECTIONS

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

WEDNESDAY, JUNE 21, 2017

Printed for the use of the Select Committee on Intelligence

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

U.S. GOVERNMENT PUBLISHING OFFICE
26–125 PDF WASHINGTON : 2017

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

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

RICHARD BURR, North Carolina, *Chairman*
MARK R. WARNER, Virginia, *Vice Chairman*

JAMES E. RISCH, Idaho
MARCO RUBIO, Florida
SUSAN COLLINS, Maine
ROY BLUNT, Missouri
JAMES LANKFORD, Oklahoma
TOM COTTON, Arkansas
JOHN CORNYN, Texas

DIANNE FEINSTEIN, California
RON WYDEN, Oregon
MARTIN HEINRICH, New Mexico
ANGUS KING, Maine
JOE MANCHIN III, West Virginia
KAMALA HARRIS, California

MITCH MCCONNELL, Kentucky, *Ex Officio*
CHUCK SCHUMER, New York, *Ex Officio*
JOHN MCCAIN, Arizona, *Ex Officio*
JACK REED, Rhode Island, *Ex Officio*

CHRIS JOYNER, *Staff Director*
MICHAEL CASEY, *Minority Staff Director*
KELSEY STROUD BAILEY, *Chief Clerk*

CONTENTS

JUNE 21, 2017

OPENING STATEMENTS

WITNESSES

SUPPLEMENTAL MATERIAL

RUSSIAN INTERFERENCE IN THE 2016 U.S. ELECTIONS

WEDNESDAY, JUNE 21, 2017

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 9:32 a.m. in Room SH–216, Hart Senate Office Building, Hon. Richard Burr (Chairman of the Committee) presiding.

Committee Members Present: Senators Burr, Warner, Risch, Rubio, Collins, Blunt, Lankford, Cotton, Cornyn, Feinstein, Wyden, Heinrich, King, Manchin, Harris, and Reed.

OPENING STATEMENT OF HON. RICHARD BURR, CHAIRMAN, A U.S. SENATOR FROM NORTH CAROLINA

Chairman BURR. I'd like to call the hearing to order.

Today the Committee convenes its sixth open hearing of 2017, to further examine Russia's interference in the 2016 elections. This is yet another opportunity for the Committee and the American people to drill down on this vitally important topic.

In 2016, a hostile foreign power reached down to the State and local levels to touch voter data. It employed relatively sophisticated cyber tools and capabilities and helped Moscow to potentially build detailed knowledge of how our elections work. It was also another example of Russian efforts to interfere into a democracy with the goal of undermining our system. In 2016, we were woefully unprepared to defend and respond and I'm hopeful that we will not be caught flatfooted again.

Our witnesses are here to tell us more about what happened in 2016, what that tells us about Russian intentions, and what we should expect in 2018 and 2020. I'm deeply concerned that if we do not work in lockstep with the states to secure our elections, we could be here in two or four years talking about a much worse crisis.

The hearing will feature two panels. The first panel will include expert witnesses from DHS and FBI to discuss Russian intervention in 2016 elections and U.S. government efforts to mitigate the threat. The second panel will include witnesses from the Illinois State Board of Elections, the National Association of State Election Directors, the National Association of Secretaries of States, and an expert on election security to give us their on-the-ground perspective on how Federal resources might be brought to bear on this very important issue.

For our first panel, I'd like to welcome our witnesses today: Dr. Samuel Liles, Acting Director of Cyber Division within the Office of Intelligence and Analysis at the Department of Homeland Security; Jeanette Manfra, Acting Deputy Under Secretary, National Protection and Programs Directorate, also at DHS.

And Jeanette, I think I told you next time you came I did not want "Acting" in front of your name. So now I've publicly said that to everybody at DHS. Hopefully next time that will be removed.

And Bill Priestap. Bill's the Assistant Director for Counterintelligence Division at the Federal Bureau of Investigation.

Bill, I want to thank you for the help that you have personally provided to the investigative staff of this Committee as we've worked through so far over five and a half months of our investigation into the 2016 elections.

As you're well aware, this Committee is in the midst of a comprehensive investigation on the specific issue: the extent to which the Russian government under the direction of President Putin conducted intelligence activities, also known as Russian active measures, targeted at the 2016 U.S. elections. The intelligence community assesses that, while Russian influence obtained and maintained access to elements of multiple U.S. State and local election boards, those systems were not involved in vote tallying.

During the first panel, I would like to address the depth and the breadth of Russian government cyber activities during the 2016 election cycle, the efforts of the U.S. government to defend against these intrusions, and the steps that DHS and FBI are taking to preserve the foundation of our democracy's free and fair elections in 2018 and beyond.

I thank all three of our first witnesses. I turn to the Vice Chairman.

OPENING STATEMENT OF HON. MARK WARNER, A U.S. SENATOR FROM VIRGINIA

Vice Chairman WARNER. Thank you, Mr. Chairman, and welcome to the witnesses. And, Bill, thank you again for all the work you've done with us.

We all know that in January the entire intelligence community reached the unanimous conclusion that Russia took extraordinary steps to intervene in our 2016 Presidential elections. Russia's interference in our elections in 2016 I believe was a watershed moment in our political history. This was one of the most significant events I think any of us on this dais will be asked to address in our time as Senators. And only with a robust and comprehensive response will we be able to protect our democratic processes from even more dramatic incursions in the future.

Much of what the Russians did at this point, I think at least in this room, is—was well known: spreading fake news, flooding social media, hacking personal e-mails and leaking them for maximum political benefit. Without firing a shot and at minimal cost, Russia sowed chaos in our political system and undermined faith in our democratic process. And as we've heard from earlier witnesses, sometimes that was aided by certain candidates in terms of their comments about the legitimacy of our democratic processes.

Less well understood, though, is the intelligence community's conclusion that they also secured and maintained access to elements of multiple U.S. State and local electoral boards. Now, again, as the Chairman has said, there's no reason to doubt the validity of the vote totals in the 2016 election. However, DHS and the FBI have confirmed—and I'm going to come back to this repeatedly—only two intrusions into the voter registration databases, in both Arizona and Illinois, even though no data was modified or deleted in those two states.

At the same time, we've seen published reports that literally dozens—I've seen one published report that actually said 39 states—were potentially attacked. Certainly it's good news that the attempts in 2016 did not change the results of that election. But the bad news is this will not be their last attempt. And I'm deeply concerned about the danger posed by future interference in our elections and attempts by Russia to undermine confidence in our whole electoral system.

We saw Russian—we saw recently—and this was just not happening here, obviously—we saw recently Russian attempts to interfere in the elections in France. And I thank the Chairman that next week we'll be having a hearing on some of these Russian efforts in Europe. We can be sure that Russian hackers and trolls will continue to refine their tactics in the future, especially if there's no penalty for these malicious attacks.

That's again, one reason I think that the Senate voted so overwhelmingly last week, and I thank all my colleagues for that 97–2 vote, to strengthen our sanctions on Russia. I hope that that action sends a strong message to Mr. Putin that there will be a heavy price to pay for attacks against the fundamental core of our democratic system.

Make no mistake, it's likely that we'll see more of these attacks not just in America, but against our partners. I heard this morning coming in on the radio that the Russians are already actively engaged in the German election cycle, which takes place this fall.

Now, some might say, "Well, why the urgency?" I can assure you, you know, we have elections in 2018, but in my home State of Virginia we have statewide elections this year. So this needs a sense of urgency. The American electoral election process, the machinery, the Election Day manpower, the actual counting and reporting, primarily is a local and State responsibility. And in many states, including my own, we have a very decentralized approach, which can be both a strength and a weakness.

In Virginia, for instance, decentralization helps deter large-scale hacking or manipulation because our system is so diffuse. But Virginia localities use more than a dozen different types of voting machines, none of which are connected to the Internet while in use, but we have a number of machine-read machines, so that the tabulations actually could be broken into on an individual machine basis.

All this makes large cyber attacks on electoral systems, because of the diffusion, more difficult. But it also makes maintaining consistent, coordinated cyber defenses more challenging as well.

Furthermore, states may be vulnerable when it comes to the defense of voter registration and voter history databases. That's why

I strongly believe that the threat requires us to harden our cyber defenses and to thoroughly educate the American public about the danger.

Yesterday, I wrote to the Secretary of Homeland Security. I urged DHS to work closely with State and local election officials to disclose publicly—and I emphasize, publicly—which states were targeted. Not to embarrass any states, but how can we put the American public on notice when we've only revealed two states, yet we have public reports that there are literally dozens? That makes absolutely no sense.

I know it is the position of DHS that since the states were victims, it is their responsibility. But I cannot believe if this was an attack on physical infrastructure in a variety of states, there wouldn't be a more coordinated response.

We are not making our country safer if we don't make sure that all Americans realize the breadth and the extent of what the Russians did in 2016 and, frankly, if we don't get our act together, what they will do in an even more dramatic form in 2018 and 2020. And candidly, the idea of this kind of bureaucratic "Well, it's not my responsibility, not my job" I don't believe is an acceptable decision.

So, I'm going to hope from our witnesses, particularly our DHS witnesses, that we hear a plan on how we can get more information into the bloodstream, how we can make sure that we have better best practices, so that all states are doing what's needed. I'm not urging or suggesting that in any way the Federal Government intervenes in what is a local and State responsibility. But to not put all Americans on notice and to have the number of states that were hacked into or attempted to be hacked into still kept secret is just crazy in my mind.

So, my hope is that we will get some answers. I do want to thank the fact that in January DHS did designate the Nation's electoral infrastructure as critical infrastructure. That's important. But if we call it critical infrastructure but then don't tell the public how many states were attacked or potentially how many could be attacked in the next cycle, I don't think we get to where we need to be.

So, we're going to see more of this. This is the new normal. I appreciate the Chairman for holding this hearing and I'm going to look forward very much to getting my questions answered.

Thank you.

Chairman BURR. Thank you, Vice Chairman.

With that, Dr. Liles, I understand you're going to go first. The floor is yours.

STATEMENT OF SAM LILES, Ph.D., ACTING DIRECTOR, CYBER DIVISION, OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY

Dr. LILES. Chairman Burr, Ranking Member Warner, and distinguished members of the Committee, thank you for the invitation to be here. My name is Sam Liles. I represent the Cyber Analysis Division of the Department of Homeland Security's Office of Intelligence and Analysis. Our mission is to produce cyber-focused intelligence, information, and analysis, represent our operational part-

ners like the NCCIC to the intelligence community, coordinate and collaborate on IC products, and share intelligence and information with our customers at the lowest classification possible. We are a team of dedicated analysts who take threats to the critical infrastructure of the United States seriously.

I'd like to begin by clarifying and characterizing the threat we observed to the election infrastructure in the 2016 election. Prior to the election, we had no indication that adversaries or criminals were planning cyber operations against the U.S. election infrastructure that would change the outcome of the coming U.S. election.

However, throughout spring and early summer 2016, we and others in the IC began to find indications that the Russian government was responsible for widely reported compromises and leaks of e-mails from U.S. political figures and institutions. As awareness of these activities grew, DHS began in August of 2016 to receive reports of cyber-enabled scanning and probing of election-related infrastructure in some states.

From that point on, I&A began working to gather, analyze, and share additional information about the threat. I&A participated in red team events, looking at all possible scenarios, collaborated and co-authored production with other intelligence community members and the National Intelligence Council. We provided direct support to the Department's operational cyber center, the National Cyber Security and Communications Integration Center, and worked hand-in-hand with the State and local partners to share threat information related to their networks.

By late September, we determined that Internet-connected election-related networks in 21 states were potentially targeted by Russian government cyber actors. It is important to note that none of these systems were involved in vote tallying. Our understanding of that targeting, augmented by further classified reporting, is that's still consistent with the scale and scope.

This activity is best characterized as hackers attempting to use commonly available cyber tools to exploit known system vulnerabilities. The vast majority of the activity we observed was indicative of simple scanning for vulnerabilities, analogous to somebody walking down the street and looking to see if you are home.

A small number of systems were unsuccessfully exploited, as though somebody had rattled the doorknob but was unable to get in, so to speak. Finally, a small number of the networks were successfully exploited. They made it through the door.

Based on the activity we observed, DHS made a series of assessments. We started out with, we had no indication prior to the election that adversaries were planning cyber operations against election infrastructure that would change the outcome of the 2016 election. We also assessed that multiple checks and redundancies in U.S. election infrastructures, including diversity of systems, non-Internet-connected voting machines, pre-election testing, and processes for media, campaign, and election officials to check, audit, and validate the results, all these made it likely that cyber manipulation of the U.S. election systems intended to change the outcome of the national election would be detected.

We also, finally, assessed that the types of systems Russian actors targeted or compromised were not involved in vote tallying.

While we continue to evaluate any and all new available information, DHS has not altered any of these prior assessments. Having characterized the threat as we observed it, I'll stop there to allow my NPPD colleague Jeanette Manfra to talk more about how DHS is working with election systems to enhance security and resiliency.

I look forward to answering your questions.

Chairman BURR. Thank you.

Ms. Manfra.

STATEMENT OF JEANETTE MANFRA, ACTING DIRECTOR AND UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Ms. MANFRA. Thank you, sir. Chairman Burr, Vice Chairman Warner, members of this Committee: thank you for today's opportunity to represent the men and women that serve in the Department of Homeland Security.

Today I'm here to discuss the Department's mission to reduce and eliminate threats to the Nation's critical physical and cyber infrastructure, specifically as it relates to our election.

Our Nation's cyber infrastructure is under constant attack. In 2016, we saw cyber operations directed against U.S. election infrastructure and political entities. As awareness of these activities grew, DHS and its partners provided actionable information and capabilities to help election officials identify and mitigate vulnerabilities on their networks.

Actionable information led to detections of potentially malicious activity affecting Internet-connected election-related networks, potentially targeted by Russian cyber actors in multiple states. When we became aware of detected activity, we worked with the affected entity to understand if a successful intrusion had in fact occurred.

Many of these detections represented potentially malicious vulnerability scanning activity, not successful intrusions. This activity, in partnership with these potential victims and targets, enhanced our situational awareness of the threat and further informed our engagement with State and local election officials across the country.

Given the vital role that elections have in a free and democratic society, on January 26 of this year the former Secretary of Homeland Security established election infrastructure as a critical infrastructure sub-sector. As such, DHS is leading Federal efforts to partner with State and local election officials, as well as private sector vendors, to formalize the prioritization of voluntary security-related assistance and to ensure that we have the communications channels and protocols, as Senator Warner discussed, to ensure that election officials receive information in a timely manner and that we understand how to jointly respond to incidents.

Election infrastructure now receives cybersecurity and infrastructure protection assistance similar to what is provided to other critical infrastructure, such as financial institutions and electric utilities.

Our election system is run by State and local governments in thousands of jurisdictions across the country. Importantly, State

and local officials have already been working individually and collectively to reduce risks and ensure the integrity of their elections. As threat actors become increasingly sophisticated, DHS stands in partnership to support their efforts.

Safeguarding and securing cyber space is a core mission at DHS. Through our National Cybersecurity and Communications Center, or NCCC, DHS assists State and local customers such as election officials as part of our daily operations. Such assistance is completely voluntary. It does not entail regulation or Federal oversight. Our role is limited to support.

In this role, we offer three types of assistance: assessments, information, and incident response. For the most part, DHS has offered two kinds of assistance to State and local officials: first, the cyber hygiene service for Internet-facing systems provides a recurring report identifying vulnerabilities and mitigation recommendations. Second, our cybersecurity experts can go on site to conduct risk and vulnerability assessments and provide recommendations to the owners of those systems for how best to reduce the risk to their networks.

DHS continues to share actionable information on cyber threats and incidents through multiple means. For example, we publish best practices for securing voter registration databases and addressing potential threats to election systems. We share cyber threat indicators and other analysis that network defenders can use to secure their systems.

We partner with the multistate Information Sharing and Analysis Center to provide threat and vulnerability information to State and local officials. This organization is partially grant-funded by DHS and has representatives that sit on our NCCC floor and can interact with our analysts and operators on a 24/7 basis. They can also receive information through our field-based personnel stationed throughout the country and in partnership with the FBI.

Finally, we provide incident response assistance at request to help State and local officials identify and remediate any possible cyber incidents. In the case of an attempted compromise affecting election infrastructure, we will share that technical information with other states to assist their ability to defend their own systems from similar malicious activity.

Moving forward, we must recognize that the nature of risk facing our election infrastructure will continue to evolve. With the establishment of an election infrastructure sub-sector, DHS is working with stakeholders to establish these appropriate coordinating councils and our mechanisms to engage with them. These will formalize our mechanisms for collaboration and ensure long-term sustainability of this partnership. We will lead the Federal efforts to support election officials with security and resilience efforts.

Before closing, I want to reiterate that we do have confidence in the overall integrity of our electoral system because our voting infrastructure is fundamentally resilient. It is diverse, subject to local control, and has many checks and balances built in. As the risk environment evolves, the Department will continue to support State and local partners by providing information and offering assistance.

Thank you very much for the opportunity to testify, and I look forward to any questions.

[The prepared statement of Ms. Manfra follows:]

TESTIMONY

OF

JEANETTE MANFRA
ACTING DEPUTY UNDER SECRETARY FOR CYBERSECURITY AND COMMUNICATIONS
NATIONAL PROTECTION AND PROGRAMS DIRECTORATE
U.S. DEPARTMENT OF HOMELAND SECURITY

DR. SAMUEL LILES
ACTING DIRECTOR, CYBER DIVISION
OFFICE OF INTELLIGENCE AND ANALYSIS
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE
THE

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE
WASHINGTON, D.C.

ADDRESSING THREATS TO ELECTION INFRASTRUCTURE

JUNE 21, 2017

Chairman Burr, Vice Chairman Warner, members of this Committee, thank you for the invitation to be here and to represent the men and women that serve in the Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A) and the National Protection and Programs Directorate (NPPD).

Given the vital role that elections play in a free and democratic society, on January 6, 2017, the Secretary of Homeland Security determined that election infrastructure should be designated as a critical infrastructure subsector. With the establishment of an Election Infrastructure subsector within the existing Government Facilities sector, DHS and its Federal partners have been formalizing the prioritization of cybersecurity assistance and protections for owners and operators of election infrastructure similar to those provided to a range of other critical infrastructure entities, such as financial institutions and electric utilities. Participation in the subsector is voluntary, and the establishment of a subsector does not create federal regulatory authority. Elections continue to be governed by state and local officials, but with additional prioritized effort by the Federal Government to provide voluntary security assistance.

As the Secretary noted to Congress last month, "we know that our Nation's cyber systems are under constant attack." Our testimony today will provide DHS's unclassified assessment of cyber operations directed against the U.S. election infrastructure and political entities during the 2016 elections, but not the overall Russian influence campaign covered in the January 2017 declassified Intelligence Community (IC) Assessment. Our testimony will also outline DHS's efforts to help enhance the security of election infrastructure operated by state and local jurisdictions around the country.

Assessing the Threat

Throughout spring and early summer 2016, the U.S. IC warned that the Russian government was responsible for the compromises and leaks of emails from U.S. political figures and institutions. This activity was part of a decade-long campaign of cyber-enabled operations directed at the U.S. Government and its citizens. As awareness of these activities grew, DHS began in August 2016 to receive reports of cyber-enabled scanning and probing of election-related infrastructure in some states. Some of this activity appeared to originate from servers operated by a Russian company. In addition to these reports and other classified information obtained during the period, DHS also received an unclassified Federal Bureau of Investigation bulletin that described a July 2016 compromise of a State Board of Elections website. The bulletin identified specific tactics and indicators and asked recipients to check their systems for similar activity. It also provided mitigation recommendations for state and local governments. DHS and its partners shared this unclassified information—specifically information regarding targeting of voter registration systems—with state and local governments to further increase awareness of the threat.

Within the Federal Government, DHS, through I&A and NPPD's National Cybersecurity and Communications Integration Center (NCCIC), began coordinating robustly with the Election Assistance Commission, the IC, and law enforcement partners. Among non-Federal partners, NPPD and I&A engaged state and local officials, as well as relevant private sector entities, to assess the scale and scope of malicious cyber activity potentially targeting the U.S. election

infrastructure. In addition to working directly with state and local officials, we partnered with stakeholders like the Multi-State Information Sharing and Analysis Center (MS-ISAC) to analyze relevant cyber data, the National Association of Secretaries of State, and the National Association of State Election Directors. We also leveraged our field personnel deployed around the country, inclusive of Intelligence Officers deployed in state and major urban area fusion centers, Cybersecurity Advisors and Protective Security Advisors located across the country, and Department of Justice field personnel, to help further facilitate information sharing and enhance outreach. Throughout September, that engagement paid off in terms of identifying suspicious and malicious cyber activity targeting the U.S. election infrastructure. A body of knowledge grew throughout the summer and fall about suspected Russian government cyber activities, indicators, and understanding that helped drive collection, investigations, and incident response activities.

One comprehensive intelligence report published by I&A in early October cataloged suspicious activity we observed on state government networks across the country. This initial look, largely based on suspected malicious tactics and infrastructure, helped inform a body of reporting directly related to election infrastructure. While not a definitive source in identifying individual activity attributed to Russian government cyber actors, it established that Internet-connected election-related networks, including websites, in 21 states were potentially targeted by Russian government cyber actors. Although we've refined our understanding of individual targeted networks, supported by classified reporting, the scale and scope noted in that October 2016 report still generally characterizes our observations: a small number of networks were successfully compromised, there were a larger number of states where attempts to compromise networks were unsuccessful, and there were an even greater number of states where only preparatory activity like scanning was observed.

With respect to our processes, the IC has noted before that the nature of cyberspace makes attribution of cyber operations difficult, but not impossible. In partnership with members of the IC, DHS applied IC analytic tradecraft techniques to reach a series of judgments about whether these events were isolated incidents, who was the likely perpetrator, that perpetrator's possible motivations, and whether a foreign government had a role in ordering or leading the operation. Using the Department's distinctive view of domestic information and intelligence reporting, our final assessment is based on an evaluation of each incident by the capabilities and tactics employed, the infrastructure used by malicious cyber actors, characteristics of the victimized networks, and adversary capability and intent.

In September, our products at the classified and unclassified levels reported that we had no indication that adversaries or criminals were planning cyber operations against the U.S. election infrastructure that would change the outcome of the coming U.S. election. Further, we assessed that multiple checks and redundancies in U.S. election infrastructure—including diversity of systems, non-Internet connected voting machines, pre-election testing, and processes for media, campaign, and election officials to check, audit, and validate results—make it likely that cyber manipulation of U.S. election systems intended to change the outcome of a national election would be detected.

During that period, we assessed that cyber operations targeting election infrastructure could be intended or used to undermine public confidence in electoral processes and potentially the outcome. This analysis supported an October 7, 2016, statement from then Secretary of Homeland Security and Director of National Intelligence that highlighted Russian cyber activities. This triggered further outreach to share threat information and offer voluntary services to assess cybersecurity of election infrastructure and processes.

The declassified January 2017 IC Assessment, "Assessing Russian Activities and Intentions in Recent U.S. Elections," captured our assessment of the Russian activity, identifying that "Russian intelligence obtained and maintained access to elements of multiple U.S. state or local electoral boards." Additionally, "DHS assesse[d] that the types of systems Russian actors targeted or compromised were not involved in vote tallying."[1] As we continue to judge any and all newly available information, DHS has not altered any of those prior assessments.

Looking ahead to future election cycles, with a recognition that the work to enhance election infrastructure security and resiliency is already under way, we assess that multiple elements of election infrastructure remain potentially vulnerable to cyber intrusions, and that multiple cyber actors may have an interest in targeting such infrastructure. The risk to U.S. computer-enabled election systems varies from county to county, between types of devices used, and among processes used by polling stations.

We continue to assess that mounting widespread cyber operations against U.S. voting machines at a level sufficient to affect a national election would require a multiyear effort with significant human and information technology resources available only to a nation-state. The level of effort and scale required to change the outcome of a national election, however, would make it nearly impossible to avoid detection.

As with other developments in the overall cyber environment, the propagation of disruptive technologies has the ability to disrupt electoral processes. For example, targeted intrusions against individual voter registration databases remain possible. With illicit access, manipulation of voter data or disruptions to their availability may impact a voter's ability to vote on Election Day. Most but not all jurisdictions, however, still rely on paper voter rolls or electronic poll books that are not connected in real-time to voter registration databases, which limited the possible impacts in 2016.

Whether a cyber operation intended to disrupt or alter the vote is successful or not, DHS remains concerned that cyber operations targeting election infrastructure could be intended to undermine public confidence. For instance, although we assess the impact of an intrusion into a vote tabulation system would likely be contained to the manipulation of unofficial Election Night reporting results and not impact the certified outcome, such an operation could undermine public confidence in the results.

Three major elements of DHS's intelligence operations were key to enhancing our awareness and understanding of the threat: integration of intelligence with operational DHS

[1] (U) National Intelligence Council, ICA 2017-01, 5 January 2017, (U) Assessing Russian Activities and Intentions in Recent U.S. Elections.

components, collaboration with IC members, and partnership with state and local governments. I&A's co-location of intelligence personnel with the NCCIC was key to enhancing the quality of information shared with customers and partners. Robust collaboration with other members of the IC helped appropriately coalesce domestic and foreign intelligence issues – a collaboration that continues to pay dividends across analysis of threats to U.S. critical infrastructure. Finally, the ability to use deployed field staff to leverage already established relationships also aided in gathering key information that shaped I&A's understanding of the threat environment.

Enhancing Security for Future Elections

Based on our assessment of activity observed, DHS is engaged with stakeholders across the spectrum to increase awareness of potential vulnerabilities and enhance security of U.S. election infrastructure. DHS continues to work with a diverse set of stakeholders to plan, prepare, and mitigate risk to the election infrastructure. Our election process is governed and administered by state and local election officials in thousands of jurisdictions across the country. These officials manage election infrastructure and ensure its security on a day-to-day basis. State and local 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 existing, ongoing engagements, DHS is working to enhance efforts to secure their election systems.

Increasingly, the nation's election infrastructure leverages information technology for efficiency and convenience. Like other systems, reliance on digital technologies introduces new cybersecurity risks. DHS's NCCIC helps stakeholders in federal departments and agencies, state and local governments, and the private sector to manage their 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.

Addressing cybersecurity challenges and helping our customers assess their cybersecurity risk is not new for DHS. We have three sets of cybersecurity customers: federal civilian agencies; state local, tribal, and territorial governments; and the private sector. Assistance includes three lines of business to support these customers: information sharing, best practices, and technical assistance. Support to state and local customers, such as election officials, is part of our daily operations.

NPPD shares actionable information about electoral infrastructure incidents through direct outreach to state and local governments and through the Multi-State Information Sharing and Analysis Center (MS-ISAC), enhancing situational awareness and providing election officials with the information needed to protect themselves from similar incidents. The MS-ISAC was created by DHS over a decade ago and is partially grant-funded by NPPD. The MS-ISAC composition is restricted to state and local government entities. It has representatives co-located with the NCCIC to enable regular collaboration and access to information and services for state chief information officers. All states are members of the MS-ISAC.

During the 2016 election cycle, and in future elections, NPPD offered and will continue to offer voluntary assistance from the NCCIC to state and local election officials and authorities interested in securing their infrastructure. The NCCIC provides this same assistance on an ongoing basis to public and private sector partners upon request.

Establishment of coordinating councils for election infrastructure owners and operators. DHS is working collaboratively with election officials and vendors of election infrastructure to establish coordinating councils that will be used to develop a physical and cyber security and resilience strategy for the Election Infrastructure subsector and define how the Federal government will work with election officials and vendors going forward. The coordinating councils will also be used to regularly share information on relevant threats and vulnerabilities quickly and efficiently so that owners and operators can manage their risk. Historically, DHS has not had active engagement directly with the state and local election community, so we're working on broadening and deepening those relationships, identifying requirements, and educating on our capabilities.

Through engagements with state and local election officials, including working through the Sector Coordinating Council, DHS actively promotes a range of services to include:

Cyber hygiene service for Internet-facing systems: This voluntary service is conducted remotely, after which DHS can provide state and local officials with a report identifying vulnerabilities and mitigation recommendations to improve the cybersecurity of systems connected to the Internet, such as online voter registration systems, election night reporting systems, and other Internet-connected election management systems.

Risk and vulnerability assessments: These assessments are more thorough and done on-site by DHS cybersecurity experts. They typically require two to three weeks and include a wide range of vulnerability testing services, focused on both internal and external systems. When DHS conducts these assessments, we provide a full report of vulnerabilities and recommended mitigations following the testing. These assessments are available on a limited, first-come, first-served basis.

Incident Response Assistance: We encourage state and local election officials to report suspected malicious cyber activity to the NCCIC. On request, the NCCIC can provide on-site assistance in identifying and remediating a cyber incident. Information reported to the NCCIC 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 states to assist their ability to defend their own systems from similar malicious activity.

Information sharing: DHS will continue to share relevant information on cyber incidents through multiple means. The NCCIC works with the MS-ISAC. Election officials can connect with their state Chief Information Officer or the MS-ISAC directly as one way to benefit from this partnership and rapidly receive information they can use to protect their systems. State election officials may also receive incident information directly from the NCCIC.

Classified information sharing: DHS provides classified briefings to cleared stakeholders upon request, and as appropriate and necessary.

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

Physical and protective security tools, training, and resources: DHS provides advice 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. Officials can also contact a local DHS Protective Security Advisor for access to DHS resources.

In closing, we want to reiterate that the fundamental right of all citizens to be heard by having their vote accurately counted is at the core of our American values. Ensuring the integrity of our electoral process is a vital national interest and one of our highest priorities as citizens in a democratic society. We have confidence in the overall integrity of our electoral system. Our voting infrastructure is diverse, subject to local control, and has many checks and balances built in. As the threat environment evolves, the Department will continue to work with state and local partners to enhance our understanding of the threat and 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 testify, and we look forward to your questions.

Chairman BURR. Thank you very much.
Mr. Priestap.

STATEMENT OF BILL PRIESTAP, ASSISTANT DIRECTOR, COUNTERINTELLIGENCE DIVISION, FEDERAL BUREAU OF INVESTIGATION

Mr. PRIESTAP. Good morning. Chairman Burr, Vice Chairman Warner, and members of the Committee: Thank you for the opportunity to appear before you today. My statement for the record has been submitted. And so, rather than restating it, I'd like to step back and provide you a description of the broader threat as I see it.

My understanding begins by asking one question: What does Russia want? As you well know, during the Cold War the Soviet Union was one of the world's two great powers. However, in the early 1990's it collapsed and lost power, stature, and much territory. In a 2005 speech, Vladimir Putin referred to this as a major catastrophe. The Soviet Union's collapse left the U.S. as the sole superpower.

Since then, Russia has substantially rebuilt, but it hasn't been able to fully regain its former status or its former territory. The U.S. is too strong and has too many alliances for Russia to want a military conflict with us. Therefore, hoping to regain its prior stature, Russia has decided to try to weaken us and our allies.

One of the ways Russia has sought to do this is by influence, rather than brute force. Some people refer to Russia's activity in this regard as information warfare, because it is information that Russia uses as a weapon.

In regards to our most recent Presidential election, Russia used information to try to undermine the legitimacy of our election process. Russia sought to do this in a simple manner. They collected information via computer intrusions and via their intelligence officers and they selectively disseminated e-mails they hoped would disparage certain political figures and shed unflattering light on political processes.

They also pushed fake news and propaganda, and they used online amplifiers to spread the information to as many people as possible. One of their primary goals was to sow discord and undermine a key democratic principle, free and fair elections.

In summary, I greatly appreciate the opportunity to be here today to discuss Russia's election influence efforts. But I hope the American people will keep in mind that Russia's overall aim is to restore its relative power and prestige by eroding democratic values. In other words, its election-related activity wasn't a one-time event. Russia will continue to pose an influence threat. I look forward to your questions. Thank you.

[The prepared statement of Mr. Priestap follows:]

Department of Justice

STATEMENT OF

BILL PRIESTAP
ASSISTANT DIRECTOR
COUNTERINTELLIGENCE DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

FOR A HEARING ENTITLED

"ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT ELECTIONS"

PRESENTED

JUNE 21, 2017

Statement of
Bill Priestap
Assistant Director
Counterintelligence Division
Federal Bureau of Investigation

Before the
Select Committee on Intelligence
United States Senate

For a Hearing Entitled
"Assessing Russian Activities and Intentions in Recent Elections"

Presented
June 21, 2017

(U) Chairman Burr, Vice Chairman Warner, and members of the Committee, thank you for the opportunity to appear before you today to discuss the FBI's contributions to the early 2017 Intelligence Community Assessment, or "ICA," entitled "Assessing Russian Activities and Intentions in Recent Elections."

(U) As the Committee is well aware, the ICA was a joint effort between the Office of the Director of National Intelligence, the CIA, the National Security Agency ("NSA"), and the FBI, in collaboration with the Department of Homeland Security ("DHS") and other U.S. Government stakeholders. In light of the interagency nature of this product — consistent with interagency agreements on the ICA — I will speak only to portions of the ICA as to which the FBI made substantial contributions in sourcing or analysis. As the Committee and the American Public are aware, the full version of the ICA is highly classified and derived from exceptionally sensitive sources and methods. Nonetheless, I am pleased to be here today to discuss the unclassified version of the report and the FBI's findings and contributions.

(U) Russia's 2016 Presidential election influence effort was its boldest to date in the United States. Moscow employed a multi-faceted approach intended to undermine confidence in our democratic process. Russia's activities included efforts to discredit Secretary Clinton and to publicly contrast her unfavorably with President Trump. This Russian effort included the weaponization of stolen cyber information, the use of Russia's English-language state media as a strategic messaging platform, and the mobilization of social media bots and trolls to spread disinformation and amplify Russian messaging. The FBI has not made an assessment of any impact that the Russian activities might have had on the outcome of the 2016 election; instead, I am here to discuss Russia's activities and the importance of combating them.

(U) The FBI's direct contributions to the ICA included FBI collection and analysis that attributed cyberattacks against U.S. political institutions and state election infrastructure specifically to the Russian Intelligence Services. We also provided historic insight into prior Russian active

measures targeting our elections. The FBI was afforded access to our partners' collection to complete the ICA, access that we gladly reciprocated to ensure that the joint team drafting the report benefitted from the entire Intelligence Community's insights into these matters.

(U) One of the FBI's primary strengths in contributing to the ICA was our history investigating Russia's intelligence operations within the United States. As articulated in the ICA, reckoning with Russian efforts to influence our elections or political processes is not a new challenge.

(U) Traditionally, these influence efforts leveraged forged documents, newspaper placements, and other publications to smear candidates who advocated positions contrary to Russia's strategic interests. Following the Cold War, Russian intelligence efforts related to U.S. elections focused primarily on foreign intelligence collection intended to help Russian leaders understand a new Administration's plans and priorities.

(U) The FBI also brought insights and expertise to the ICA's judgments on Russian cyber activities. While I cannot, in this setting, discuss the FBI's sensitive sources and methods that underpinned our judgments, we welcome our continued engagement with the Committee and its staff on these matters in closed session. I will highlight the attribution to the Russian General Staff Main Intelligence Directorate ("GRU") of the cyber intrusions into the Democratic National Committee ("DNC") and the correlation of data exfiltrated from the DNC to the information later posted on DCLeaks.com.

(U) Beyond the specific scope of the ICA, I am pleased to be joined by my colleagues from DHS, with whom we closely collaborated in the run-up to the election to protect our voting infrastructure and ensure American confidence in our election. Thank you for this opportunity to testify. I look forward to your questions.

Chairman BURR. Thank you very much to all of our witnesses.

For members, we will proceed by seniority for recognition for up to five minutes, and the Chairman will tell you when you have used all your time if you proceed that far. The Chair would recognize himself for five minutes.

Yes or no, to all three of you. Most important question: Do you have any evidence that the votes themselves were changed in any way in the 2016 Presidential election?

Dr. Liles.

Dr. LILES. No, sir. There was no detected change in the vote.

Chairman BURR. Ms. Manfra.

Ms. MANFRA. No, sir.

Chairman BURR. Mr. Priestap.

Mr. PRIESTAP. No, sir.

Chairman BURR. Bill, to you. This adversary is determined. They're aggressive and they're getting more sophisticated by the day. The diversity of our election system is a strength, but the intrusions into State systems also show that Moscow is willing to put considerable resources towards an unclear result.

In 2016, we saw voter data stolen. How could Moscow potentially use that data?

Mr. PRIESTAP. They could use the data in a variety of ways. Unfortunately, in this setting I can't go into all of them. First of all, I think they took the data to understand what it consisted of, what's there, so that they can in effect better understand and plan accordingly.

And when I say "plan accordingly," plan accordingly in regards to possibly impacting future elections and/or targeting of particular individuals, but also by knowing what's there and studying it they can determine if it's it something they can manipulate or not, possibly, going forward. And there's a couple of other things that wouldn't be appropriate in this setting as well.

Chairman BURR. To any of you: You've heard the Vice Chairman talk about his frustration about publicly talking about how many states. Can you tell the American people why you can't disclose which states and the numbers?

I'll turn to Ms. Manfra first.

Ms. MANFRA. Thank you for the question, sir. There are—through the long history that the Department has in working with the private sector and State and local on critical infrastructure and cybersecurity issues, we believe it is important to protect the confidentiality that we have and the trust that we have with that community. So when the entity is a victim of a cyber incident, we believe very strongly in protecting the information around that victim.

That being said, what we can do is take the technical information that we learn from the engagement with that victim and anonymize it so it is not identified as to what that entity or individual is. We can take all the technical information and turn that around and share that broadly with whether it's the affected sector or broadly across the entire country. And we have multiple mechanisms for sharing that.

But we believe that this has been a very important key to our success in developing trusted relationships across all of these 16 critical infrastructure sectors.

Chairman BURR. Are we prepared today to say publicly how many states were targeted?

Ms. MANFRA. We, as of right now, we have evidence of 21 states, election-related systems in 21 states that were targeted.

Chairman BURR. But in no case were actual vote tallies altered in any way, shape, or form?

Ms. MANFRA. That is correct.

Chairman BURR. How did the French respond to the Russian involvement in the French elections a month ago? Is that something we followed, the Bureau? Bill?

Mr. PRIESTAP. Sir, From the Bureau's standpoint, it's something we followed from afar. We did have engagement with French officials, but I'm just not at liberty to go into what those consisted of.

Chairman BURR. Okay. We've talked about last year, Russia's intent, their target. Let's talk about next year. Let's talk about the 2017 elections in Virginia. Let's talk about the 2018 elections, Congressional and gubernatorial elections. What are we doing to prepare ourselves this November and next November?

Ms. Manfra.

Ms. MANFRA. Yes, sir. As we noted, we are taking this threat very seriously, and part of that is identifying this community as a critical infrastructure subsector. That's allowed us to prioritize and formalize the engagement with them.

Similar to the 2016 elections, we are identifying additional resources, prioritizing our engagement with them through information-sharing products, identifying, in partnership again with the State and local community, those communication protocols—how do we ensure that we can declassify information quickly should we need to and get it to the individuals that need it.

We also have committed to working with State and local officials on incident response playbooks. So how do they understand where to engage with us, where do we engage with them, and how do we—are we able to bring the entire resources of the Federal Government to bear in helping the State and local officials secure their election systems?

Chairman BURR. Great.

Vice Chairman.

Vice Chairman WARNER. Thank you for the answer at 21. 21 states is almost half the country. We've seen reports that were even higher. I concur with the Chairman that the vote totals were not changed. But can you explain to me how we're made safer by keeping the identity of 19 of those states secret from the public, since Arizona and Illinois have acknowledged they were attacked?

Dr. LILES. Well, sir, I'd bring it back to the earlier points you made about the future elections. One of the key pieces for us within I&A is our ability to work with our partners because of how our collection mechanisms work. It's built on a high level of trust——

Vice Chairman WARNER. If this was water systems or power systems, would the public be safer by not knowing that their water system or power system in their respective State was attacked?

Ms. MANFRA. Sir, I can—for other sectors we apply the same principles. When we do have a victim of an incident in the electric sector or the water sector, we do keep the name of that entity confidential. Some of these sectors do have breach reporting requirements that requires the victims——

Vice Chairman WARNER. Are all 21 of the states that were attacked, are they aware they were attacked?

Ms. MANFRA. All of the system owners within those states are aware of the targeting, yes, sir.

Vice Chairman WARNER. At the State level, you could have local registrars and other local officials that there may have been an attempt to penetrate at the State level and you may have local registrars in the respective states that would not even know that their State had been the subject of Russian activities?

Ms. MANFRA. We are currently working with State election officials to ensure communication between the local and the State officials.

Vice Chairman WARNER. But at this moment in time, there may be a number of State and local election officials that don't know their states were targeted in 2016, is that right?

Ms. MANFRA. The owners of the systems that were targeted do know that they were targeted——

Vice Chairman WARNER. The owners may know, but because we have a decentralized system many local elective—I just——

Ms. MANFRA. I cannot——

Vice Chairman WARNER [continuing]. Fundamentally disagree. I understand the notion of victimization.

Ms. MANFRA. Yes, sir.

Vice Chairman WARNER. But I do not believe our country is made safer by holding this information back from the American public. I have no interest in trying to embarrass any State, but if this—because we've seen this for too long in cyber, we've seen it in the financial industry, and others, where people simply try to sweep this under the rug and assume they'll go along their way.

When we're talking about—I go back to Dr. Liles' initial comments. We had no idea—we had no ability to predict this beforehand. We had 21 states that were tapped. We've got two that have come forward. While no election results were changed, we do know there were a number of states—perhaps you'll answer this: How many states did the Russians actually exfiltrate data, such as voter registration lists?

Ms. MANFRA. I'd prefer not to go into those details in this forum, sir. I can tell you that we're tracking 21 states that were targeted——

Vice Chairman WARNER. Do the states who had their data exfiltrated by the Russians—are they aware of that?

Ms. MANFRA. Yes, sir.

Vice Chairman WARNER. And is there any coordinated response on how we're going to prevent this going forward?

Ms. MANFRA. Yes, sir.

Vice Chairman WARNER. How do we make sure, if states are not willing to acknowledge that they had vulnerabilities, that they were subject to attack—again, we're in a brave new world here,

and I understand your position. I'm not trying to—I'm very frustrated, but I'm not—I get this notion.

But I think we need a re-examination of this policy. You know, the designation by former Secretary Johnson as critical infrastructure, what does that change in terms of how our operations are going forward? By that designation in January, I appreciated it, but what does that really mean in practical terms, in terms of assistance or information sharing?

Ms. MANFRA. What it means, it means three things, sir. The first is a statement that we do recognize that these systems are critical to the functioning of American life, and so that is an important statement.

The second is that it formalizes and sustains the Department's prioritization of engagement with this community. And the last is, it provides a particular protection for sharing of information, in particular with vendors within the election community, that allows us to have conversations to discuss vulnerabilities with potential systems, that we would not have to disclose.

Vice Chairman WARNER. I talked to Secretary Kelly last week, and I hope you'll take this, at least this Senator's message, back to him. I would like us to get more information. What I have heard today is that, there were 21 states. I appreciate that information, but within those 21 states I have no guarantee that local election officials are aware that their State system may have been attacked, number one.

Number two, we don't know how many states actually had exfiltration. And the final question is, have you seen any stoppage of the Russian activities after the election? Or are they continuing to ping and try to feel out our various election systems?

Ms. MANFRA. On the first two questions, sir, we will be happy to get back to you. I spoke to the Secretary this morning and look forward to responding to your letter. On the third question, I'll defer to the FBI.

Mr. PRIESTAP. Vice Chairman, I just can't comment on our pending investigations related to the cyber——

Vice Chairman WARNER. You can't say whether the—so, should the public take away a sense of confidence that the Russians have completely stopped, as of November of 2016, trying to interfere or tap into our electoral systems? Is that what you're saying?

Mr. PRIESTAP. That's not what I'm saying, sir. I believe the Russians will absolutely continue to try to conduct influence operations in the U.S., which will include cyber intrusions.

Vice Chairman WARNER. Thank you, Mr. Chairman.

Chairman BURR. Thank you, Vice Chairman.

To DHS and to the Bureau, a quick question; and if you can't answer it, please go back and get us an answer. Would your agency be opposed to the Chair and Vice Chair sending a letter to the 19 states that have not been publicly disclosed, a classified letter, asking them if they would consider publicly disclosing that they were a target of the last election?

Mr. PRIESTAP. Sir, I'd be happy to take that question back to my organization, but I would just add that the role your Committee is playing in regards to highlighting the Russians' aims and activities I think is critically important for this country.

The Bureau is just trying to balance what, we'll call it the messaging end of that, with doing things that hopefully don't impact what we can learn through our investigations. I know it's a fine balance, but the bottom line is you play a key role in raising awareness of that, and I thank you.

Chairman BURR. Fair concern, and if both of you would just go back and get back with us, we'll proceed from there.

Senator Risch.

Senator RISCH. Thank you much.

So that the American people can have solid confidence in what you've done, and thank you for what you've done, could you give the American people an idea—if you feel the numbers are classified and that sort of thing, you don't have to go into it—but the number of people that were involved on DHS and the FBI in this investigation? Can you give us a general idea about that? Whichever one of you want to take that question. Ms. Manfra.

Ms. MANFRA. From a DHS perspective, we did amass quite a few resources both from our intelligence and analysis and our operations analysis. To put a number on it is somewhat challenging but, you know——

Senator RISCH. Would you say it was substantial?

Ms. MANFRA. It was a substantial level of effort, yes, sir.

Senator RISCH. You're confident that you got where you wanted to go when you set out to make this investigation?

Ms. MANFRA. Yes, sir. One of our key priorities was developing relationships with that community and getting information out, whether it was to the specific victims or broader indicators that we could share. We accomplished that. We held multiple sessions. We sent over 800 indicators to the community, and so we do believe that we accomplished that. We don't want to let that down at all. We want to continue that level of effort and we intend to continue it.

Senator RISCH. And I'm focusing on not what you did after you got the information, but how you got the information. You're confident you got what you needed to appropriately advise everyone on this, what was going on?

Ms. MANFRA. Yes, sir. Yes, we did.

Senator RISCH. Mr. Priestap.

Mr. PRIESTAP. The FBI considered this a very grave threat and so we dedicated substantial resources to this effort as well.

Senator RISCH. Okay. Thank you.

To both of you, both agencies again: Everyone in this Committee knows the specificity and identity of the Russian agencies involved. Are you comfortable in identifying them here today, or do you feel—still feel that's classified?

Mr. PRIESTAP. Yeah. Other than what was mentioned in the unclassified version of the intelligence community assessment, I'd rather not go into any of those details.

Senator RISCH. Were there any of those agencies identified, any of the Russian intelligence agencies, identified in that?

Mr. PRIESTAP. It's my understanding that GRU was identified.

Senator RISCH. Homeland Security, same answer?

Dr. LILES. Yes, sir.

Senator RISCH. Okay. Thank you much.

Let me ask this question. And I come at this from a little different perspective, and I think the American people have the right to know this. From all the work that either of your agencies did, all the people involved, all the digging you did through what the Russians had done and their attempts, did you find any evidence, direct or circumstantial, to any degree, down to a scintilla of evidence, that any U.S. person colluded with, assisted, or communicated with the Russians in their efforts?

Mr. Priestap.

Mr. PRIESTAP. I'm sorry, I just can't comment on that today. That falls under the Special Counsel's purview and I have to defer to him.

Senator RISCH. Are you aware of any such evidence?

Mr. PRIESTAP. And I'm sorry, sir, I just can't comment on that.

Senator RISCH. Ms. Manfra.

Ms. MANFRA. Sorry, sir. I cannot also comment on that.

Senator RISCH. Thank you.

Thank you, Mr. Chairman.

Chairman BURR. Senator Feinstein.

Senator FEINSTEIN. Thanks very much, Mr. Chairman.

Candidly, I'm very disappointed by the testimony. I mean, we have learned a great deal and the public has learned a great deal. And it seems to me we have to deal with what we've learned.

Mr. Priestap, is that correct? You have said, and I think quite pointedly, that Russia has decided to weaken us through covert influence rather than brute force. And I think that's a correct assessment, and I thank you for having the courage to make it.

Here's a question. To the best of the FBI's knowledge, have they conducted covert influence in prior election campaigns in the United States? If so, when, what and how?

Mr. PRIESTAP. Yes, absolutely they've conducted influence operations in the past. What made this one different in many regards was of course the degree and then with what you can do through electronic systems today.

When they did it in the past, it was doing things like trying to put in biased or half-true stories, getting stories like that into the press or pamphlets that people would read, so on and so forth. The Internet has allowed Russia to do so much more today than they've ever been able to do in the past.

Senator FEINSTEIN. So you're saying prior campaigns were essentially developed to influence one campaign above another, to denigrate a candidate if she was elected and to support another candidate subtly?

Mr. PRIESTAP. Yeah, I'm saying that Russia, for years, has conducted influence operations targeting our elections, yes.

Senator FEINSTEIN. Equal to this one?

Mr. PRIESTAP. Not equal to this one. No, ma'am.

Senator FEINSTEIN. Okay, here we go. What made this one different?

Mr. PRIESTAP. Again, I think the scale, the scale and the aggressiveness of the effort, in my opinion, made this one different. And again, it's because of the electronic infrastructure, the Internet, what have you, today that allowed Russia to do things that in the past they weren't able to do.

Senator FEINSTEIN. Would you say that this effort was tailored to achieve certain goals?

Mr. PRIESTAP. Absolutely.

Senator FEINSTEIN. And what would those goals have been?

Mr. PRIESTAP. I think the primary goal in my mind was to sow discord and to try to delegitimize our free and fair election process. I also think another of their goals, which the entire United States intelligence community stands behind, was to denigrate Secretary Clinton and to try to help then—current President, Trump.

Senator FEINSTEIN. Have they done this in prior elections in which they've been involved?

Mr. PRIESTAP. Have they——

Senator FEINSTEIN. Denigrated a specific candidate and-or tried to help another candidate?

Mr. PRIESTAP. Yes, ma'am, they have.

Senator FEINSTEIN. And which elections were those?

Mr. PRIESTAP. Oh—I'm sorry. I know there—I'm sorry, I can't think of an example off the top of my head, but even though—all the way through the Cold War, up to our most recent election, in my opinion, they have tried to influence all of our elections since then, and this is a common practice.

Senator FEINSTEIN. Have they ever targeted what is admitted here today to be 21 states?

Mr. PRIESTAP. If they have, I am not aware of that. That's a—that scale is different than what I'm aware of what they tried to do in the past. So again, the scale and aggressiveness here separates this from their previous activity.

Senator FEINSTEIN. Has the FBI looked at how those states were targeted?

Mr. PRIESTAP. Absolutely, ma'am.

Senator FEINSTEIN. And what is your finding?

Mr. PRIESTAP. We have a number of investigations open in regards to that. In this setting, because they're all still pending investigations, I'd rather not go into those details.

The other thing I'd ask you to keep in mind is that we continue to learn things. So, there was some activity we were looking at prior to the election. It's not like when the election was finished our investigation stopped. So as we learn more, we share more.

Senator FEINSTEIN. Do you know if it's the intent of the FBI to make this information public at some point?

Mr. PRIESTAP. I think this gets back to an issue the Vice Chairman raised, and I guess I want to be clear on my position on it. I think it is critically important to raise awareness about Russia's aims to undermine our democracy, and then their tradecraft and how they do it.

My organization—part of understanding that tradecraft is conducting our investigations where we learn more and more about tradecraft. So we try to balance, what do we need to provide to partners so they can best protect themselves versus not interrupting our investigations if the information were to be made public.

Senator FEINSTEIN. Thank you very much.

Mr. PRIESTAP. A balancing act.

Senator FEINSTEIN. My time is up. Thank you

Chairman BURR. Thank you, Senator Feinstein.

The Vice Chairman and I have already decided that we're going to invite the Bureau in for a classified briefing to update all members on the open investigations and any that we see that might warrant, on their minds, an opening of a new investigation.

In addition, let me remind members that one of the mandates of our investigation is that we will, at the end of this, work with the Bureau and other appropriate agencies to make a public report in as great a public detail as we can our findings on Russia's involvement in our election.

So, it is the intent of the Chair, at least, to make sure that as much as we can declassify, it's done and the public gets a true understanding when we put out a final report.

Senator Rubio.

Senator RUBIO. Thank you, Mr. Chairman. And that's critically important. I think the most important thing we're going to do in this report is tell the American people how this happened, so we're prepared for the next time. And it begins, I think, by outlining what their goals were, what they tried to do, in this regard.

And we know what they tried to do, because they've done it in other countries around the world for an extensive period of time. The first is, undermine the credibility of the electoral process; to be able to say, that's not a real democracy. It's filled with all kinds of problems.

The second is to undermine the credibility of our leaders, including the person who may win. They want that person to go into office hobbled by scandal and all sorts of questions about them. And the third, ideally, in their minds, I imagine, is to be able to control the outcome in some specific instances. If they think they could, either through public messaging, or even in a worst case scenario by actually being able to manipulate the vote—which I know has now been repeatedly testified did not happen here.

And, by the way, these are not mutually exclusive. You can do all three, you can only take one. They all work in conjunction. I think you can argue that they have achieved quite a bit, if you think about the amount of time that we have been consumed in this country on this important topic and the political fissures that it's developed.

And the way I always kind of point to it—and if anyone disagrees I want you to tell me this—but, you know, we have something in American politics. It's legitimate; both sides do it. It's called opposition research. You find out about your opponent. Hopefully it's embarrassing or disqualifying information if you're the opposition research person. You package it. You leak it to a media outlet. They report it. You run ads on it.

Now, imagine being able to do that with the power of a nation state, illegally acquiring things like e-mails and being able to weaponize it by leaking, leaking it to somebody who will post that and create all sorts of noise. I think that's certainly one of the capabilities.

The other is just straight-out misinformation, right? The ability to find a site that looks like a real news place, have them run a story that isn't true, have your trolls begin to click on that story.

It rises on Facebook as a trending topic. People start to read it. By the time they figure out it isn't true, a lot of people think it is.

I remember seeing one in early fall that President Obama had outlawed the Pledge of Allegiance, and I had people texting me about it. And I knew that wasn't true, but my point is that we have people texting about it, asking if it was. It just tells you—and I don't know if that was part of that effort, or it was just somebody with too much time on their hands.

And then the third, of course, is the access to our voting systems, and obviously people talk about affecting the tallies. But just think about this. Even the news that a hacker from a foreign government could have potentially gotten into the computer system is enough to create the specter of a losing candidate arguing, the election was rigged, the election was rigged.

And because most Americans, including myself, don't fully understand all the technology that's around voting systems per se, you give that "election is rigged" kind of narrative to a troll and a fake news site, and that stuff starts to spread. And before you know it, you have the specter of a political leader in America being sworn in under the cloud of whether or not the election was stolen because vote tallies were actually changed.

So I don't know why they were probing these different systems, because obviously a lot of the information they were looking at was publicly available. You can buy it, voter rolls. Campaigns do it all the time. But I would speculate that one of the reasons potentially is because they wanted these stories to be out there, that someone had pinged into these systems, creating a specter of being able to argue at some point that the election was invalid because hackers had touched election systems in key states.

And that is why I really, truly believe, Mr. Chairman, it is so important that, to the extent possible, that part of it, the systems part, as much of it be available to the public as possible, because the only way to combat misinformation is with truth and with facts, and explain to people, and I know some of it is proprietary. I know some of it we were trying to protect methods and so forth, but it is really critical that people have confidence that when they go vote that vote is going to count and someone's not going to come in electronically and change it.

And I think they're—I just really hope we err on the side of disclosure about our systems so that people have full confidence when they go vote. Because I can tell you, I was on the ballot in November, and I remember people asking me repeatedly, is my vote going to count? I was almost afraid people wouldn't vote because they thought their vote wouldn't count. So I just hope as we move forward—I know that's not your decision to make in terms of declassifications and the like, but it is really, really, really important that Americans understand how our voting systems work, what happened, what didn't and that we be able to communicate that in real-time in the midst of an election, so that if in 2018 these reports start to emerge about our voting systems being pinged again, people aren't—we can put out enough information in October and early November so people don't have doubts.

And I know that's not your decisions to make, but I just really hope that's part of what we push on here, because I think it's critical for our future.

Chairman BURR. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman.

Let me say to the three of you, and I say it respectfully, that on the big issue, which is which states were affected by Russian hacking in 2016, the American people don't seem to be getting more information than what they already had before they showed up. We want to be sensitive to security concerns, but that question has to be answered sooner rather than later. I want to send that message in the strongest possible way.

We obviously need to know about vulnerabilities so that we can find solutions, and we need better cybersecurity to protect elections from being hacked in the first place. And that means solutions like Oregon's vote-by-mail system, that has a strong paper trail, air-gapped computers, and enough time to fix the problems if they pop up.

But now to my question. You all mentioned the January intelligence assessment, saying that the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying. Your prepared testimony today makes another point that I think that is important. You say it is likely that cyber-manipulation of U.S. election systems intended to change the outcome of a national election would be detected. So that is different than what we have heard thus far.

So I have two questions for you, Ms. Manfra, and you, Dr. Liles: What level of confidence does the Department have in its assessment that 2016 vote tallying was not targeted or compromised? And second, does that assessment apply to State and local elections?

Dr. LILES. Thank you, sir, for the question.

So, the level of effort and scale required to change the outcome of a national election would make it nearly impossible to avoid detection. This assessment is based on the diversity of systems, the need for physical access to compromise voting machines themselves, the security of pre-election testing employed by the State and local officials. There's a level, a number of standards and security protocols that are put in place. In addition, the vast majority of localities engage in logic and accuracy testing, which work to ensure voting machines are operating and tabulating as expected.

Before, during, and after the election, there has been an immense amount of media attention applied to this, which also brings in the idea of people actually watching and making sure that the election results represent what they see. And plus there's just the statistical anomalies that would be detected, so we have a very high confidence in our assessments.

Senator WYDEN. What about State and local elections? Do you have the same level of confidence?

Dr. LILES. So, from the standpoint of a nation-state actor operating against a State and local election system, we would have the same—for an Internet-connected system, we would have the same level of confidence.

Senator WYDEN. Ms. Manfra.

Ms. MANFRA. Yes, sir. And I think this also gets to Senator Rubio's point about the difficulty in the general public understanding the variety of systems that are used in our election process.

So we broke our level of engagement and concern down to a couple of different areas. The voter registration systems, which are often, usually connected to the Internet. We also were looking at the voting machines themselves, which by best practice and by the voluntary voting standards and guidelines that the Department of Commerce works with the Election Assistance Commission on, is, by best practice—those are not connected to the Internet.

Senator WYDEN. So can Homeland Security assure the public that the Department would be able to detect an attempted attack on vote tallying?

Ms. MANFRA. What I would suggest, sir, is that the ability, as has been demonstrated by security researchers, to access remotely a voting machine to manipulate that vote and then to be able to scale that across multiple different voting machines made by different vendors, would be virtually impossible to occur in an undetected way within our current election system.

Senator WYDEN. Has the Department conducted any kind of post-election forensics on the voting machines that were used in 2016?

Ms. MANFRA. We are currently engaged with many vendors of those systems to look into conducting some joint forensics with them. The vendor community is very interested in engaging with us. We have not conducted——

Senator WYDEN. So there's no—there's been no analysis yet?

Ms. MANFRA. We have not—our Department has not conducted forensics on specific voting machines.

Senator WYDEN. Do you believe it's important to do that in terms of being able to reassure Americans that there was no attack on vote tallying?

Ms. MANFRA. Sir, I would say that we do currently have voluntary standards in place that vendors are enabled—and in approximately 35 states, actually require, some level of certification of those voting machines that they are complying with those standards. We would absolutely be interested in working with vendors to conduct that level of analysis.

Senator WYDEN. Let me ask one last question. Obviously, the integrity of elections depends on a lot of people: State and local election officers, equipment vendors, third party contractors. Are you all, at Homeland Security and the FBI, confident that the Federal Government has now identified all of the potential government and private sector targets?

Ms. MANFRA. Yes, sir. I'm confident that we've identified the potential targets.

Senator WYDEN. Okay.

Thank you, Mr. Chairman.

Chairman BURR. Senator Collins.

Senator COLLINS. Mr. Priestap, let me start by saying that it's a great pleasure to see you here again. I remember back in 2003, you were detailed to the Homeland Security Committee when I was the Chairman and how helpful you were in our drafting of the In-

telligence Reform and Terrorism Prevention Act. So thank you for your continued public service.

You testified this morning and answered the question of, what does Russia want? And you said that the Russians want to undermine the legitimacy of our elections and sow the seeds of doubt among the American public.

Despite the exposure and the publicity given to the Russian's efforts in this regard, do you have any doubt at all that the Russians will continue their activities in subsequent elections?

Mr. PRIESTAP. I have no doubt. I just can't—I just don't know the scale and aggressiveness, whether they'll repeat that, if it'll be less or if it'll be more. But I have no doubt they will continue.

Senator COLLINS. Is there any evidence that the Russians have implanted malware or backdoors or other computer techniques to allow them easier access next time to our election systems?

Mr. PRIESTAP. I'm sorry, Senator. I just can't comment on that because of our pending investigations.

Senator COLLINS. Secretary Manfra, the secretaries of state who are responsible for the election systems have a pretty blistering attack on the Department of Homeland Security in the testimony that will be given later this morning. And I want to read you part of that and have you respond. They say: "Yet, nearly six months after the designation"—and they mean the designation of election systems as critical infrastructure—"and in spite of comments by DHS that they are rushing to establish election protections, no secretary of state is currently authorized to receive classified threat information that would help them to protect their election systems." Why not?

Ms. MANFRA. Thank you, ma'am, for that question. I would note that this community, the secretaries of state, and for those states where they have a State election director, is not one that the department has historically engaged with. And what we have done in the process of building the trust and learning about how they do their work and how we can assist, we have identified the need to provide clearances to that community. And so we have committed to them to work through that process between our Department and the FBI.

Senator COLLINS. Let me ask you about your own agency, which is the agency that focuses on critical infrastructure, including our election systems. Now, NPPD is not an official element of the intelligence community that would have routine access to especially sensitive classified information. So how do you know with any certainty whether you and others in the agency are read into all the relevant classified information that may exist regarding foreign threats to our critical infrastructure, including our election systems?

Ms. MANFRA. Yes, ma'am. I would say, despite the fact that we're not a part of the intelligence community and our focus is on network defense and operations, in partnership with the critical infrastructure and the Federal Government, we feel very confident that with the partnership with our own Intelligence and Analysis Division, that serves as an advocate for us within the intelligence community, as well as our direct relationships with many of those individuals in organizations such as the FBI, NSA, and others, that we

receive information quickly; And when we ask to declassify that, they are responsive. And we work through our partners at the Intelligence and Analysis Office to ensure that that happens quickly.

So is there room for improvement? Absolutely, of course. But we have the full commitment of the intelligence community to support us and get us the information that we need and our stakeholders need.

Senator COLLINS. And, finally, how many states have implemented all the best practices recommended in the document developed by DHS regarding the protection of election systems?

Ms. MANFRA. Ma'am, I'd have to get back to you on a specific number of states. I don't have that.

Senator COLLINS. Do you think most states have?

Ms. MANFRA. In our informal engagement, many of them noted that they had already adopted some of these and to the extent that they weren't they were incorporating them.

Senator COLLINS. I would ask for a response for the record.

Ms. MANFRA. Yes, ma'am.

Senator COLLINS. That's a really important point.

Chairman BURR. Senator Heinrich.

Senator HEINRICH. Mr. Priestap, I want to thank you for just how seriously you've taken this and how you've answered the questions this morning in your testimony. I think you hit the nail on the head when you said we need to step back and ask the fundamental question, what do the Russians want?

And by outlining that they want to undermine legitimacy in our system, that they want to sow discord, that they want to undermine our free and fair elections, we really have a better lens with which to understand the specifics of what happened in 2016. In your view, were the Russians successful at reaching their goals in their activities in our 2016 elections?

Mr. PRIESTAP. I don't know for certain whether the Russians would consider themselves successful. In many ways, they might argue that, because of the time and energy we're spending on this topic, maybe it's distracting us from other things. But on the other hand, exactly what this Committee is doing as far as raising awareness of their activities, their aims, for the American people, to me they've done us—in my opinion, they've done the American public a service in that regard. And so, I guess I don't know, but could argue either way.

Senator HEINRICH. Yes. I think the jury's certainly out for the future, but when you look at the amount of discord that was sown and the impact on 2016, I hope that the outcome of what we're doing here is to make sure that in 2018, and in 2020, and 2022, that by no metric will they have been successful.

Mr. Priestap, you stated, very correctly, that one of their primary goals was to delegitimize our democracy. Are are you familiar with the term "unwitting agent"?

Mr. PRIESTAP. Yes, I am.

Senator HEINRICH. Can you kind of summarize what that is for us?

Mr. PRIESTAP. In an intelligence context, it would be where an intelligence service is trying to advance certain aims and they reach out to a variety of people, some of which they might try to

convince to do certain things; and the people, person or persons they contact might actually carry those out, but for different reasons than the intelligence service that actually wanted them to carry them out. In other words, they do it unwittingly.

Senator HEINRICH. By effectively reinforcing the Russian narrative and publicly saying that our system is rigged, did then-candidate Trump, now President Trump, become what intelligence officials call an unwitting agent?

Mr. PRIESTAP. I can't give you a comment on that.

Senator HEINRICH. I don't blame you for not answering that question.

[Laughter.]

We've got about a minute 46 left. Can you talk about the relationship between the election penetration that we saw and the coincident Russian use of what Senator Rubio very aptly described of trolls, of bots, of social media, all designed to manipulate the American media cycle, and how those two things fit together?

Mr. PRIESTAP. I'm sorry. To clarify, fit together the intrusions with the——

Senator HEINRICH. What's the relationship between what they were doing in our elections from a technical point of view and what they were seeking to do in our media cycle by using trolls and bots and manipulation of the media cycles.

Mr. PRIESTAP. I guess the best way I can describe it is that this was a, my opinion, a well-planned, well-coordinated, multi-faceted attack on our election process and democracy. And while that might sound complicated, but it was actually really straightforward. They want to collect intelligence from a variety of sources, human and cyber means. They want to evaluate that intelligence, and then they want to selectively—they might selectively disseminate some of it. They might use others for more strategic discussions.

But at the end of the day it's all about collecting intelligence that would give them some type of advantage over the United States and/or attempt to influence things, and then, coordinated, well-coordinated, well-funded, diverse ways to disseminate things to hopefully influence American opinion.

Senator HEINRICH. This is a very sophisticated, highly resourced effort.

Mr. PRIESTAP. Absolutely.

Senator HEINRICH. Thank you.

Chairman BURR. Senator Blunt.

Senator BLUNT. Thank you. Thank you, Chairman.

Let's talk a little bit about once—let's start with a comment that DHS made in its written comment which says it assesses that the systems Russian actors targeted or compromised were not involved in vote tallying. Now, is that because the vote tallying systems are a whole lot harder to get into than the voter registration systems?

Ms. MANFRA. I can't make a statement as to why different systems were targeted. What we can assess is that those vote tallying systems, whether it was the machines at a kiosk that a voter uses at the polling station or the systems that are used to tally votes, were very difficult to access, and particularly to access them remotely. And then, given the level of observation for vote tallying at

every level of the process, that adds into, you know, that we would have identified issues there, and there were no identified issues. So those two are——

Senator BLUNT. Okay. I would think that if you could get into the vote tallying system and you did want to impact the outcome of an election, obviously the vote tallying system is the place to do that. And I would also suggest that all of your efforts, a lot of your efforts, should be to continue to do whatever DHS thinks they need to advise—I don't think we should centralize this system—to give advice to State and local election officials to be sure that that vote tallying system is protected at a level above other systems.

You know, the voter registration system is public information. It is generally accessible in lots of ways. It's not nearly as protected, for that reason. You have lots of input from lots of sources into that system.

And I think, Ms. Manfra, you made the point that you said that the best practice would be to not have the vote tallying system connected in any unnecessary way to the Internet. Is that right?

Ms. MANFRA. Both the kiosks themselves and vote tallying systems, to not connect them to the Internet and to also have, ideally, paper auditing trails as well.

Senator BLUNT. Well, I certainly agree with that. The paper trail is significant and I think more prevalent as people are looking at new systems. But also, I think any kind of third party monitoring—the first two parties would be the voter and the counting system—just creates another way into the system. So my advice would be that DHS doesn't want to be in a situation where somehow you're connected to all the voting systems of the country.

And Mr. Liles, I think you said the diversity of our voting system is a great strength of the system. Do you want to comment on that any more?

Dr. LILES. Yes, sir. When we were setting it as part of our red teaming activities, we looked at the diversity of the voting system as actually a great strength and the fact that there were not connected in any one kind of centralized way. So we evaluated that as—when we were looking at the risk assessment with OCIA, the Office of Cyber Intelligence Analysis—Infrastructure Analysis, we looked at that as one of the great strengths and our experts at the IC we worked with also said the same thing.

Senator BLUNT. Well, I would hope you'd continue to think about that as one of the great strengths as you look at this critical infrastructure, because every avenue for Federal monitoring is also just one more avenue for somebody else to figure out how to get into that system.

And again, the voter registration system, dramatically different in what it does. All public information accessible, printed out, given to people to use, though you are careful of what information you give and what you don't. But almost all election officials that have this system now have some way to share that with the public as a system.

There is no reason to share the security of the vote counting system with the public or to have it available or accessible. And I would hope that the DHS, or nobody else, decides that you're going

to save this system by having more avenues, more avenues into the system.

Ms. MANFRA. Absolutely not, sir. We're fully supportive of the voluntary standards process, and we are engaging with that process with our experts, and we continue, again, with the voluntary partnership with the State and local. And we intend to continue that.

Senator BLUNT. Thank you.

Thank you, Mr. Chairman.

Chairman BURR. Senator King.

Senator KING. Thank you, Mr. Chairman.

Starting with a couple of short questions, Mr. Priestap. Number one, you've stated this was a very grave threat, that Russia—the attempts to probe and upset our local election systems. Any doubt it was the Russians?

Mr. PRIESTAP. No, sir.

Senator KING. Any doubt that they'll be back?

Mr. PRIESTAP. No, sir.

Senator KING. To our DHS witnesses, have the 21 states that you've mentioned, that we know where we had this happen, been notified officially?

Ms. MANFRA. Sir, the owners of the systems within those 21 states have been notified.

Senator KING. How about the election officials in those states?

Ms. MANFRA. We are working to ensure that election officials as well understand. I'll have to get back to you on whether all 21 states——

Senator KING. Have you had a conference of all State election officials, secretaries of state, here in Washington on this issue?

Ms. MANFRA. I have had at least two teleconferences; and in-person conferences, we will be engaging with them in July, I believe.

Senator KING. Well, I would urge you to put some urgency on this. We've got another election coming in 18 months, and if we're talking about systems and registration rolls, the time is going by. So I believe this is, as we've already heard characterized, is a very grave threat. It's going to be back and shame on us if we're not prepared.

Ms. MANFRA. Yes, sir. We have biweekly—every other week, we hold a teleconference with all relevant election officials. The national associations that represent those individuals have nominated bipartisan individuals to engage with us on a regular basis.

This is of the utmost urgency for the Department and this government to ensure that we have better protections going forward, and the community, the election community, is similarly committed and has been so for years.

Senator KING. And just to be clear, nobody's talking about a Federal takeover of local election systems or Federal rules. What we're talking about is technical assistance and information and perhaps some funding at some point?

Ms. MANFRA. Sir, this is similar to our engagement with all critical infrastructure sectors, whether it's the electrical sector, the nuclear sector, the financial sector, is completely voluntary and it is about this Department providing information both to potential vic-

tims, but to all network defenders, to ensure that they have access to what we have access to and can better defend themselves.

Senator KING. Thank you.

Mr. Liles, I'll take issue with something that you said, that we have a national election and it was just too large, too diverse, to really crack. We don't have a national election. What we have are 50 State elections. And each election in the states can depend upon a certain number of counties. There are probably 500 people within the sound of my voice who could tell you which ten counties in the United States will determine the next Presidential election.

And so you really—a sophisticated actor could hack a Presidential election simply by focusing on particular counties. Senator Rubio I'm sure remembers Dade County in the year 2000 and the significance that had to determining who the next President of the United States was.

So I don't think it works to just say, oh, it's a big system and the diversity will protect us, because it really is county by county, city by city, State by State, and a sophisticated actor, which the Russians are, could easily determine where to direct their attack. So I don't want to rely on the diversity.

Second, a separate point is, what do we recommend? And we've talked about paper backups. The Dutch just had an election where they just decided to make it all paper and count the ballots by hand, for this very reason. So what would you tell my elections clerk in Brunswick, Maine, Ms. Manfra, would be the top three things he or she should think about in protecting themselves in this situation?

Ms. MANFRA. Sir, I would say to, first, as previous Senators mentioned, prioritize the security of your voting machines and the vote tallying system, ensure that they are not connected to the Internet, even if that is enabled on those particular devices.

Second, ensure that you have an auditing process in place where you can identify anomalies throughout the process, educate polling workers to look for suspicious activity, for example.

Senator KING. But doesn't auditing mean a paper trail, a paper backup?

Ms. MANFRA. Yes, sir. I would recommend a paper backup.

Senator KING. And one of the worrisome things, again, on the issue of the national, we talk about how diverse it is, but aren't we seeing a consolidation in terms of the vendors who are producing these machines?

Ms. MANFRA. Yes, sir. It is my understanding that we are seeing some consolidation in the vendor community. Again, many of them are committed and have engaged on the voluntary voting standards and guidelines, which partly include security.

We will be updating those security guidelines in 2018. And yes, while there is some concern about consolidation, we do look forward to engaging with them, and as of now they are a very engaged community.

Senator KING. I think this aspect of this question that this Committee is looking at is one of the most important, and frankly one of the most daunting, because we pretty well determined that they weren't successful in changing tallies and changing votes, but they weren't doing what they did in at least 21 states for fun. And they

are going to be back, and they're going to be back with knowledge and information that they didn't have before.

So I commend you for your attention to this and certainly hope that this is treated with the absolute utmost urgency.

Thank you, Mr. Chairman.

Chairman BURR. Senator Lankford.

Senator LANKFORD. Thank you, Mr. Chairman.

Thanks to all of you for being here as well today.

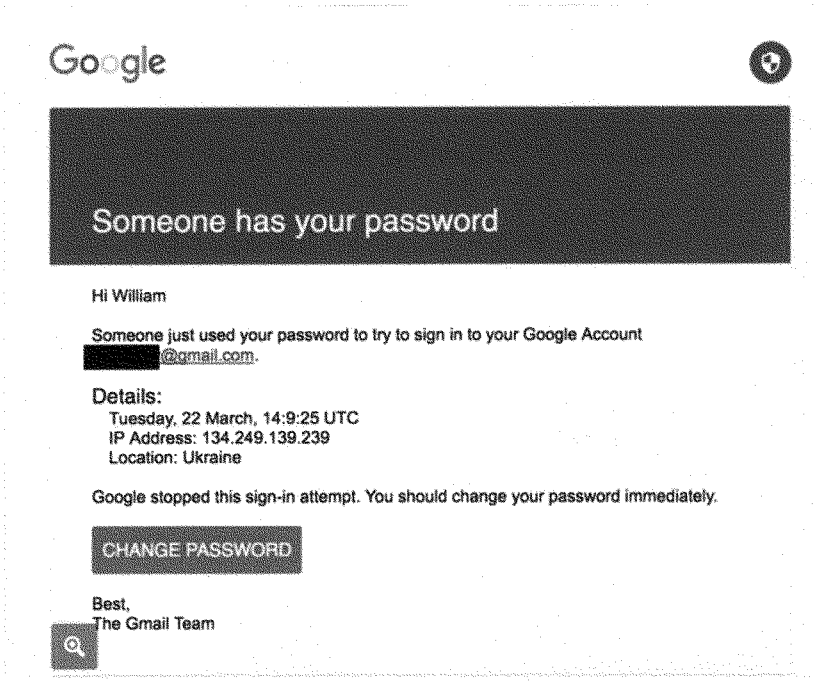
To Senator King just as a heads up, there are some states that are like that. For 25 years the Oklahoma election system has had a paper ballot and an optical scan and it's been a very good back-up for us. We quickly count because of the optical scan, but we're able to go back and verify because of paper.

This is such a big deal and it's such an ongoing conversation that I'm actually in two simultaneous hearings today I'm running back and forth with. In the Department of Homeland Security and what we're dealing with State elections and with State systems, is also happening in the HSGAC hearing that I'm also at, including my own Oklahoma CIO that's there testifying today on this same issue, how we are protecting State systems, State elections and what's happening.

I brought this with me today. You all are probably—this group is very, very familiar with this e-mail. This is the famous e-mail that Billy Rinehart got from the DNC while he happened to be on vacation. He was out in Hawaii enjoying some quality time away from his work at the DNC, and he gets an e-mail from Google, it appears, that says someone has used your password, someone just tried to sign in to your Google account; sent it to him and told him someone tried to do it from the Ukraine; and recommended that he go in and change his password immediately.

[The material referred to follows:]

Sen. Lankford's Visual Aid



Google

Someone has your password

Hi William

Someone just used your password to try to sign in to your Google Account [redacted]@gmail.com.

Details:
Tuesday, 22 March, 14:9:25 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

A screenshot of the phishing email that Billy Rinehart clicked on, unknowingly giving Russian hackers access to his account. The New York Times has redacted Mr. Rinehart's email address.

Source: "The Perfect Weapon: How Russian Cyberpower Invaded the US." New York Times, Dec. 13, 2016

Senator LANKFORD. Which, as the New York Times reported, he groggily at 4:00 a.m., when he saw that e-mail was frustrated by it, went in, clicked on the link, changed his password and went back to bed. But what he actually did was just gave the Russian government access to the DNC, and then it took off from there.

Multiple other staff members of the DNC got an e-mail that looked just like this. Now, everyone who has a Google account, will know that really looks like a Google account warning. It looked like the real thing. When you hovered over the "change password," it showed a Google account connection where it was going to, but it wasn't. It was going to the Russians.

About 91 percent, my understanding is, about 91 percent of the hacks that come into different systems, start with a spear phish attack that looks just like this.

So let's talk about, in practical terms, for our State election folks and what happens in my State and other states. First for you, Mr. Priestap. How does Russia identify a potential target? Because this is not just a random e-mail that came to him. This was targeted directly at him, to his address. It looked very real, because they knew who he was and where he works. So, how were the Russians that savvy to be able to track this person and how does this work in the future for an election system for a State?

Mr. PRIESTAP. So I can't go into great detail in this forum, but I'd say what intelligent services do, not just Russia there, is they're looking for vulnerabilities. That would begin in the cyber sense with computer vulnerabilities.

As far as targeting specific individuals, I don't know all the facts surrounding that e-mail and all the e-mails that were sent, but my guess is they didn't just send it to one person. They sent it the email like that to a whole variety, just hoping that one would click on it.

Senator LANKFORD. Right. But how are they getting that information? Are they going to their website, for instance, and gathering all the e-mails for it? I'm trying to figure out, are they tracking individuals to get more information, so they get something that looks like something they would click on?

Mr. PRIESTAP. Yes. You hit on it, but a whole variety of ways. They might get it through reviewing open source material, either online or otherwise. But they also collect a lot of information through human means as well.

Senator LANKFORD. So, Ms. Manfra, let me ask you this question. When someone at any location clicks on a link like this, what access to information do they get typically?

Ms. MANFRA. Well, sir, it depends on the system itself. I imagine that's probably a frustrating response. But given the—and I think this is important for the public to understand. As the threat evolves, they're going to continue as we educate the public, don't click on certain things. Look at, you know, make sure you know the sender, for instance, before you click on it, and as our defense gets better the offense is going to look for other means.

And so we look, you know, in this case, ideally, we want people to look and see what is it that they're actually clicking on before they click it. Some organizations choose to say when an individual clicks on that link, they choose to not allow that to go to that des-

ignation, because they know it's suspicious or they have some mechanisms in place to put that into a container and look at it. Other organizations don't take those steps, and it really depends on your risk management and the technical control that you put in place.

Senator LANKFORD. Let me ask you a quick question. Who has primary responsibility for Federal election integrity? Which agency is the prime mover in that? Obviously, states oversee their own, but which Federal entity is working with the State to say they're the prime person or the prime agency to do it?

Ms. MANFRA. For election cybersecurity, our Department, in coordination with the FBI and others, is leading the partnership with State and locals.

Senator LANKFORD. Great. Thank you.

Chairman BURR. Senator Manchin.

Senator MANCHIN. Thank you, Mr. Chairman.

And thank all of you for your appearance here today and your testimony. Being a former secretary of state of my great State of West Virginia, and also being a former governor, my utmost concern was voter fraud. Every time that we would have a report of a fraud, I would see the election participation decrease the next election cycle, thinking their vote didn't count.

Is there any reason at all that any person that has the knowledge that you all have, or anyone that you've—on our Committee here, from the intelligence community, would give you any doubt that Russia was involved, and Russia was very much involved with the intent of doing harm to our election process, as far as the confidence level that voters would have? Do any of you have any concerns whatsoever, any doubts, that the Russians were behind this and involved in a higher level than ever? All three of you.

Mr. PRIESTAP. No, no doubt from the FBI's end as far as Russia's involvement.

Senator MANCHIN. And you've all interacted with all the intelligence community, right?

Mr. PRIESTAP. Yes, sir.

Ms. MANFRA. Similar, sir. I have no doubt.

Mr. LILES. No, sir.

Senator MANCHIN. So nobody. There's not an American right now that should have a reasonable doubt whatsoever that the Russians were involved.

Were all 50 states notified on Russia's intentions and activities during the 2016 election cycle? Had you all put an alert out? So if I'd have been secretary of state in charge of my elections in West Virginia, would you have notified me to be on the lookout?

Ms. MANFRA. Sir, I can discuss our products that we put out and I'll defer to the FBI on what they put out. We did put out products, not public products, but we did put out products, primarily leveraging our Multi-State Information Sharing Analysis Center, which has connections to all 50 states CIOs.

And we engaged with the Election Assistance Commission and other national associations that represent those individuals to ensure that we were able to reach—again, this was a community that we had not historically engaged with, and so we relied on those, and we did put out multiple products prior to the election.

Senator MANCHIN. And you're really not sure if these national associations, the secretaries of states, dispersed that information, put everybody on high alert?

Ms. MANFRA. I believe that they did, sir. We also held a conference call where all 50 secretaries of state or an election director if the secretary of state didn't have that responsibility, in August, in September, and again in October, both high-level engagement and network defense products.

Senator MANCHIN. And if I could ask this questions to whoever, maybe Mr. Priestap. What was Russia's intention, and do you think they were successful in what they desired to do, even though they didn't alter—as you all have said, you can see no alterations of the election results. Do you believe that it had an effect in this election outcome of this 2016 election?

Mr. PRIESTAP. As far as Russia's intention, again, the broader being to undermine democracy and one of the ways they sought to do this, of course, here was to undermine the legitimacy of our free and fair election.

Senator MANCHIN. Do you believe they were successful in the outcome?

Mr. PRIESTAP. No, I—the FBI doesn't look at that as far as did Russia achieve its aims in that regard.

Senator MANCHIN. Let me ask this question. Are there counteractions the U.S. can take to subvert or punish the Russians for what they have done and their intention to continue? And what's your opinion of the sanctions that we have placed on Russia?

Mr. PRIESTAP. As you know, the FBI doesn't do policy. I'm here today to provide you an overview of the threat picture, at least as I understand and see it. But obviously the U.S. government did take action post-election in regards to making a number of Russian officials——

Senator MANCHIN. Have you seen them subside at all any of their activities since we have taken some actions?

Mr. PRIESTAP. Subside? They have less people to carry out their activities, so it's certainly had an impact on the number of people.

Senator MANCHIN. And finally, with the few seconds I have left, have we shared this with our allies, our European allies, who are going through election processes, and have they seen the same intervention in their election process that we have seen from the Russians in ours?

Mr. PRIESTAP. Sure. I can't speak for DHS, but the FBI is sharing this information with our allies, absolutely.

Senator MANCHIN. How about DHS?

Ms. MANFRA. We are also sharing information with our allies.

Senator MANCHIN. Are they seeing a high—an overaggressive, high activity, from the Russians that they haven't seen at this level before, such as we did during the 2016 election?

Dr. LILES. Sir, there is media reporting that suggests that. We don't have direct government-to-government relationships from a DHS perspective. There is definitely media reporting that they're seeing an increased activity.

Senator MANCHIN. Thank you.

Chairman BURR. Senator Cotton.

Senator COTTON. Thank you all for your appearance today.

Mr. Priestap, in response to Mr. Heinrich's question about whether Donald Trump had become an unwitting agent of Russia and their efforts to sow discord and discontent about our elections, you said that you declined to answer, which is understandable.

Let's look at this from a different perspective. Since her election defeat, Hillary Clinton has blamed her loss on the Russians, Vladimir Putin, the FBI, Jim Comey, fake news, WikiLeaks, Twitter, Facebook, and, my personal favorite, content farms in Macedonia. In her blaming her loss on these actors, has Hillary Clinton become an unwitting agent of Russians' goals in the United States?

Mr. PRIESTAP. And I'm sorry, sir, but I'd rather not comment. It's just something——

Senator COTTON. I understand. I just wanted to point out that you can look at it from two different——

Mr. PRIESTAP [continuing]. It's just something I haven't given any thoughts to.

Senator COTTON. Let's turn to other matters, then. Would you advise states and localities in the conduct of their elections or, more broadly, in their government services not to use or not to do business with Kaspersky Labs, companies that do business with Kaspersky, or companies that use Kaspersky products in their systems?

Mr. PRIESTAP. Sir, I can't really comment on that in this setting.

Senator COTTON. Miss Manfra, would you advise them not to use Kaspersky products?

Ms. MANFRA. I can also not comment on that in this forum, sir.

Senator COTTON. I don't even have to ask, Dr. Liles. You're reaching for your microphone.

Dr. LILES. Yes, sir. I can't comment either.

Senator COTTON. Okay. Senator Risch says he'll answer, but I'll let him speak for himself at a later time.

Mr. Priestap, we've talked a lot about Russia's intent and activities in our elections, but I think it's important that the American people realize that it goes much farther than just elections and the 2016 campaign, as well. Isn't it true that Russian cyber actors have been probing U.S. critical infrastructure for years?

Mr. PRIESTAP. Yes, sir. I can't go into specifics, but they probe a lot of things of critical importance to this country.

Senator COTTON. And as the head of counterintelligence, you write in your statement, that quote, "Russia's 2016 Presidential election influence effort was its boldest to date in the United States," which implies there have been previous efforts. You also say that the FBI had to strengthen the intelligence community assessment because of our history investigating Russia's intelligence operations within the United States. Both of which suggest that this keeps you pretty busy in your portfolio at counterintelligence, is that right?

Mr. PRIESTAP. That's correct.

Senator COTTON. And this Russian intelligence threat is not just a cyber threat, either. It also is a threat from traditional human intelligence, or what a layman might call spies, is that right?

Mr. PRIESTAP. Yes, sir.

Senator COTTON. Do so-called diplomats who work down out of the Russian embassy in Washington, D.C., have the requirement to

notify our State Department in advance if they plan to travel more than 25 miles, and give that notification 48 hours in advance?

Mr. PRIESTAP. They do.

Senator COTTON. And the State Department's supposed to notify the FBI in advance of those travel arrangements, correct?

Mr. PRIESTAP. Yes.

Senator COTTON. Is it true that the Russian nationals often fail to give that notification at all, or they give it at, say, 4:55 on a Friday afternoon before a weekend trip?

Mr. PRIESTAP. I'd prefer not to go into those details here, but—I'll leave it at that.

Senator COTTON. Does it complicate you and your agents' efforts to conduct your counterintelligence mission to have Russian nationals wandering around the country more than 25 miles outside their duty assignment?

Mr. PRIESTAP. Sure. If that were to happen, that would absolutely complicate our efforts.

Senator COTTON. The Secretary of Defense recently indicated at an Armed Services Committee hearing that Russia is in violation of something called the Open Skies Treaty, a treaty we have with Russia and other nations that allow us to overfly their territory and take pictures and they do the same here. Do we see so-called Russian diplomats traveling to places that are in conjunction with Open Skies flights that Russia's conducting in this country?

Mr. PRIESTAP. I'm sorry, I just can't comment on that here.

Senator COTTON. Okay. Last summer, an American diplomat in Moscow was brutally assaulted on the doorstep of our embassy in Moscow. Did we take any steps to retaliate against Russia for that assault in Moscow? Did we declare persona non grata any of their so-called diplomats here in the United States?

Mr. PRIESTAP. If I recall correctly, we didn't immediately do anything in that regard.

Senator COTTON. Okay. This Committee passed unanimously in Committee last year something that just passed as part of the omnibus spending bill in April a provision that would require, one, the State Department to notify the FBI of any requests for Russian diplomats to travel more than 25 miles outside their embassy and to report violations to you.

It further requires the State Department to report those violations regularly to this Committee. What's the status of that provision now that it's been in law for about two months? Is the State Department cooperating more fully with you?

Mr. PRIESTAP. I guess I'd rather not comment on that here. We're still working through the implementation of that.

Senator COTTON. Well, I certainly hope they start.

Thank you.

Chairman BURR. Senator Harris.

Senator HARRIS. Thank you.

Ms. Manfra, you mentioned that you notified the owners. I'm not clear on who the owners are. Are they the vendors?

Ms. MANFRA. What I meant to clarify is in some case it may not be the secretary of state or the state election director who owns that particular system. So in some cases it could be a locality or a vendor.

Senator HARRIS. So is there a policy of who should be notified when you suspect that there's a threat?

Ms. MANFRA. We are working through that policy with the secretaries of state. That is one of the commitments that we made to them, and election directors, in order to ensure that they have appropriate information, while preserving the confidentiality of the victim publicly.

Senator HARRIS. And can you tell us which states—in which states you notified the vendor instead of notifying the secretary of state?

Ms. MANFRA. We keep the vendor information confidential as well.

Senator HARRIS. Are there states that you notified where you did not notify the person who was elected by the people of that State to oversee elections?

Ms. MANFRA. I don't believe that's the case, but I will get back to you with a definitive answer.

Senator HARRIS. And how specific was the warning that you sent? What exactly is it that you notified the states or the vendors of?

Ms. MANFRA. Depending on the scenario and the information that we had—and more generally, what we do is when we get classified information we look to declassify as much as possible to enable——

Senator HARRIS. Let's talk about the election, yes.

Ms. MANFRA. So for this particular one, what we took was technical information that we had, that we believed was suspicious, and that was emanating from Russia, and was targeting their system. We asked them to look at their system. We asked—and this was part of the broader dissemination as well—we asked all states to look at their system, to identify whether they had an intrusion or whether they blocked it. In most cases, they blocked it.

Senator HARRIS. Do you have a copy with you of the notification you sent to these various vendors or states?

Ms. MANFRA. I do not, ma'am, but we can get back to you.

Senator HARRIS. Okay, and will you provide this Committee with a copy of the notification you sent to those states or vendors?

Ms. MANFRA. Many of them were done in person, but what I can show you is the technical information. That was also rolled up in the information that we published in December, but I can show you what we provided to the states and localities.

Senator HARRIS. And did you notify each of them the same way? Or did you tailor the notification to each State?

Ms. MANFRA. We tailor the notification. It's a process for all victim or potential victim notifications, us and the FBI. So sometimes it may be an FBI field agent that goes out there, sometimes it may be a Department official that goes out there.

Senator HARRIS. Okay. So in your follow-up to the Committee, please provide us with specifically who notified each State, and then who in that State was notified, the vendor or the State election official, and also what specifically they were notified of.

In 2007, California worked with leading security researchers—the secretary of state at the time was Deborah Bowen—and they instituted some of the best practices, we believe, for election secu-

rity. And my understanding is that it is considered a gold standard. So my question is, does DHS have the technical capability and authority to coordinate a study like that for all of the states?

Ms. MANFRA. We do have the technical capability and authority to conduct those sorts of studies, ma'am, yes.

Senator HARRIS. Have you pursued that as a viable option to help the states do everything they can to secure their systems?

Ms. MANFRA. That is one of the areas that we're considering, yes, ma'am.

Senator HARRIS. So have you taken a look at that study that was commissioned in California in 2007? And if not, I'd encourage that you do.

Ms. MANFRA. I have not personally, but I will read it, ma'am.

Senator HARRIS. And I'm also concerned that the Federal Government does not have all the information it needs in these situations where there's been a breach. Is there any requirement that a State notify the Federal Government when they suspect there's been a breach?

Ms. MANFRA. No, ma'am.

Senator HARRIS. And in terms of the American public and voters in each of these states, can you tell me is there any requirement that the State notify its residents when the State suspects there may be a breach?

Ms. MANFRA. I cannot comment. I know that multiple states have different sunshine laws, etcetera, that apply to data breaches within the State, so I couldn't make a general statement about what their requirements are at the State level.

Senator HARRIS. And do any of you have any thoughts about whether there should be such requirements, both in terms of states reporting to the Federal Government and also states reporting to their own residents and citizens about any breaches of their election system?

Ms. MANFRA. Required data breach reporting is a complicated area. We prefer, and we've had a fair amount of success with, voluntary reporting and partnerships, but we'd be happy to work with your staff in further understanding how that might apply here.

Senator HARRIS. Okay, I appreciate that. Any other thoughts as we think about how we can improve notification and sharing of information?

[No response.]

No. Okay, thank you.

Chairman BURR. Before I move to Senator Reed, let me just say that, since a number of members have questioned the agencies, especially those that are here, and the sharing with Congress of the investigation, I'll just say that the Chair and the Vice Chair were briefed at the earliest possible time and continued to be briefed throughout the process, and then it was opened up to all the members of the Committee. I'm not sure that I had ever shared that with everybody, but I just want to make sure that everybody's aware of that.

Senator Reed.

Senator REED. Thanks very much, Mr. Chairman.

Thank you very much, ladies and gentlemen. Let's start with Mr. Priestap. Are you aware of any direction or guidance from Presi-

dent Trump to conduct this investigation about the Russian interest in our elections?

Mr. PRIESTAP. Sir, I can't comment on that. It could be potentially related to things under the Special Counsel's purview.

Senator REED. Thank you.

Ms. Manfra, in terms of the Department of Homeland Security, are you aware of any direction by the President to conduct these types of operations or your investigations?

Ms. MANFRA. Sir, to clarify the question, direction from the President to——

Senator REED. That the President of the United States has directed that the Department of Homeland Security and other Federal agencies conduct the activities that you're conducting, essentially an investigation into the Russian hacking in the election.

Ms. MANFRA. I can't comment on the President's directions specifically, but our Secretary is committed to understanding what happened, ensuring that we are better protected in the future, so our activities are fully supported.

Senator REED. He has not communicated that this is at the direction of the President of the United States?

Ms. MANFRA. No, sir.

Senator REED. Dr. Liles.

Dr. LILES. Sir, this comes directly—the IC has been working on this for quite a while, and the Secretary has completely supported it.

Senator REED. But again, no——

Dr. LILES. Nothing from the President directly, sir.

Senator REED. Thank you.

I thought Senator King raised some very interesting issues in terms of most elections, national elections, as much you like to think about it, particularly from Rhode Island, are not decided in certain states, but decided even in certain cities and counties, which raised an interesting question. You were very assertive about that you'd be able to diagnose an intrusion that was altering voter—votes, literally. When could you do that? Within weeks of an election, on Election Day, after Election Day?

Dr. LILES. Sir, from an IC perspective, the way we would do that is by looking at the threats themselves that were targeting the specific entities. And the other element that we would look at is, as the reporting itself was coming in, if there was any statistical anomalies in what we were seeing.

And I'd also point out that we're talking about Internet-connected systems here, and not all of the key counties that you would represent would be those Internet-connected systems.

Senator REED. But, effectively, I think what you've said is that you'd really have to wait for confirmation until the results started coming in on Election Day, which raises the issue of, even if you detect it on Election Day, what do we do? The votes have already been cast.

Are you—is anyone planning on—what's the—what reaction we take? How do we notify people? What are—what steps do we take?

Dr. LILES. I'd have to defer that to others.

Ms. MANFRA. Yes, sir. And I do want to clarify, when we say that that activity would be difficult to detect, it would be—or difficult

to go on undetected, it would—that we're discussing both at the polling station or the jurisdiction, that it would be hard for somebody to do that without anybody, not necessarily that the Department would have that immediate insight.

And to answer your question, yes, that is absolutely something that is a part of our planning and what we would look forward to partnering with the State and local officials on understanding.

Senator REED. So we're, again, about 18 months away from election. We have to be able to develop, not technical infrastructure, but an organizational infrastructure that could react, maybe on very short notice, to discovery that actual votes were being tampered. Is that accurate?

Ms. MANFRA. Absolutely, sir. It is both technical and organizational.

Senator REED. And do you think there's enough emphasis in terms of the resources and support to do that, the collaboration? You got 50 states and among those states many of the voting jurisdictions are not at the State level; they're the city and town. Are we taking it serious enough? I guess that's the issue.

Ms. MANFRA. Absolutely, sir. This is one of our highest priorities. And I would also note that we're not just looking ahead to 2018, as election officials remind me routinely that elections are conducted on a regular basis. And so—highest priority, sir. Yes.

Senator REED. Let me ask, Mr. Priestap. If I've pronounced it incorrectly, forgive me. But you testified today, and your colleagues, that information was exfiltrated by the Russians. What type of information was taken and what could it be used for?

Mr. PRIESTAP. Yes. I don't want to get into the details of what victim information was taken. Again, we've got a variety of pending investigations. But again, it could be used for a variety of purposes. It could have been taken to understand what's in those systems. It could have been taken to use to try to target—learn more about individuals, so that they could be targeted.

It could have been taken in a way to then publicize, just to send a message that a foreign adversary has the ability to take things and to sow doubt in our voters' minds.

Senator REED. Let me ask you this question, as a judgment. Given the activities that the Russians have deployed, significant resources, constant effort over—as you, the intelligence community—probably a decade, do you think they have a better grasp of the vulnerabilities of the American voting system than you have?

Mr. PRIESTAP. I hope not. I think it's an excellent question and I can—well, first of all, I hope not and I don't think so. But if they did, I don't think they do any more.

Senator REED. Thank you very much.

Chairman BURR. Thank you, Senator Reed.

Before we move to the second panel, one last question, Mr. Priestap, for you. Is there any evidence that the attempt to penetrate the DNC was for the purposes of launching this election year intrusion process that they went on? Or was this at the time one of multiple fishing expeditions that existed by Russian actors in the United States?

Mr. PRIESTAP. In my opinion, it was one of many efforts. You'd call it a fishing expedition, but to determine, again, what's out

there, what intelligence can they collect. So they don't go after one place. They go after lots of places and then——

Chairman BURR. Tens? Hundreds? Thousands?

Mr. PRIESTAP. Hundreds, at least hundreds.

Chairman BURR. Okay.

I want to wrap up the first panel with just a slight recap. I think you have thoroughly covered that there's no question that Russia carried out attacks on State election systems. No vote tallies were affected or affected the outcome of the elections. Russia continues to engage in exploitation of the U.S. elections process and elections are now considered a critical infrastructure, which is extremely important and does bring some interesting potential new guidelines that might apply to other areas of critical infrastructure that we have not thought of because of the autonomy of each individual State and the control within their State of their election systems.

So I'm sure this will be further discussed as the appropriate committees talk about Federal jurisdiction, where that extends to. And clearly, I think it's this Committee's responsibility as we wrap up our investigation to hand off to that Committee somewhat of a road map from what we've learned are areas that we need to address, and we will work very closely with DHS and with the Bureau as we do that.

With that, I will dismiss the first panel and call up the second panel.

[Pause.]

Chairman BURR. I'd like to call the second panel to order, and ask those visitors to please take their seats. As we move into our second panel this morning, our hearing is shifting from a Federal Government focus to a State-level focus. During this second panel, we'll gain insight into the experiences of the states in 2016, as well as hear about efforts to maintain election security moving forward.

For our second panel, I'd like to welcome our witnesses: the Honorable Connie Lawson, President-elect of the National Association of Secretaries of State and the Secretary of State of Indiana; Michael Haas, the Midwest Regional Representative to the National Association of State Election Directors and the Administrator of the Wisconsin Election Commission; Steve Sandvoss, Executive Director of the Illinois State Board of Elections; and Dr. J. Alex Halderman, Professor of Computer Science and Engineering, University of Michigan.

Thank you all for being here. Collectively, you bring a wealth of knowledge and a depth of understanding of our State election systems, potential vulnerabilities of our voting process and procedures, and the mitigation measures we need to take at the State level to protect the foundation of American democracy.

In January of this year, then-Secretary of Homeland Security Jeh Johnson designated the election infrastructure used in Federal elections as a component of U.S. critical infrastructure. DHS stated that the designation established election infrastructure as a priority within the national infrastructure protection plan. It enabled the Department to prioritize our cybersecurity assistance to State and local election officials for those who requested it, and made it publicly known that the election infrastructure enjoys all the bene-

fits and protections of critical infrastructure that the U.S. government has to offer.

Some of your colleagues objected to this designation, seeing it as Federal Government interference. Today I'd like to hear your views on this specifically, but more broadly how the states and the Federal Government can best work together. I'm a proud defender of states' rights but this could easily be a moment of "divided we fall." We must set aside our suspicions and see this for what it is, an opportunity to unite against a common threat. Together, we can bring considerable resources to bear and keep the election system safe.

Again, I'd like to thank our witnesses for being here, and at this time I'd turn to the Vice Chairman for any comments he might make.

The Vice Chairman doesn't have any.

I will assume, Mr. Haas, that by some process you have been elected to go first, unless there is an agreement—which—where are we going to start?

Mr. HAAS. Actually, I think we were going to defer to Secretary Lawson to start, if that's okay with the Chair.

Chairman BURR. Madam Secretary, you are recognized.

STATEMENT OF CONNIE LAWSON, PRESIDENT-ELECT, NATIONAL ASSOCIATION OF SECRETARIES OF STATE, AND SECRETARY OF STATE, STATE OF INDIANA

Ms. LAWSON. Well, good morning, Chairman Burr and Vice Chairman Warner and distinguished members of the Committee. I want to thank you for the chance to appear before you today. It's an honor to represent the Nation's secretaries of state, 40 of whom serve as chief State election officials.

I am Connie Lawson, Indiana Secretary of State, and I'm also President-Elect of the bipartisan National Association of Secretaries of State. I'm here to discuss our capacity to secure State and locally-run elections from very significant and persistent nation state cyber threats.

With statewide elections in New Jersey and Virginia this year and many more contests to follow in 2018, I want to assure you and all Americans that election officials across the United States are taking cybersecurity very seriously. First and foremost, this hearing offers a chance to separate facts from fiction regarding the 2016 presidential election. As noted many times, we have seen no evidence that vote casting or counting was subject to manipulation in any State or locality, nor do we have any reason to question the results.

Just a quick summary of what we know about documented foreign targeting of State and local election systems. In the 2016 election cycle, as confirmed by the Department of Homeland Security, no major cybersecurity issues were reported on Election Day, November 8. Last summer, our intelligence agencies found that up to 20 State networks had been probed by entities essentially rattling the door knobs to check for unlocked doors. Foreign-based hackers were able to gain access to voter registration systems in Arizona and Illinois, prompting the FBI to warn State election offices to increase their election security measures for the November election.

In more recent days, we've learned from a TOP SECRET NSA report that the identity of a company providing voter registration support services in several states was compromised.

Of course, it's gravely concerning that election officials have only recently learned about the threats outlined in the leaked NSA report, especially given the fact that the former DHS Secretary Jeh Johnson repeatedly told my colleagues and I that no specific or credible threats existed in the fall of 2016. It is unclear why our intelligence agencies would withhold timely and specific threat information from election officials.

I have every confidence that other panelists will address voting equipment risk and conceptual attack scenarios for you today. But I want to emphasize some systemic safeguards that we have against cyber attackers. Our system is complex and decentralized, with a great deal of agility and low levels of connectivity. Even within states, much diversity can exist from one locality to the next. This autonomy serves as a check on the capabilities of nefarious actors.

I also want to mention the recent designation of election systems as critical infrastructure. Real issues exist with the designation, including a lack of clear parameters around the order, which currently provides DHS and other Federal agencies with a large amount of unchecked executive authority over our election's process. At no time between August of 2016 and January of 2017 did NASS and its members ever have a thorough discussion with DHS on what the designation means.

Threat-sharing had been touted as a key justification for the designation. Yet, nearly six months later, no secretary of state is currently authorized to receive classified threat information from our intelligence agencies.

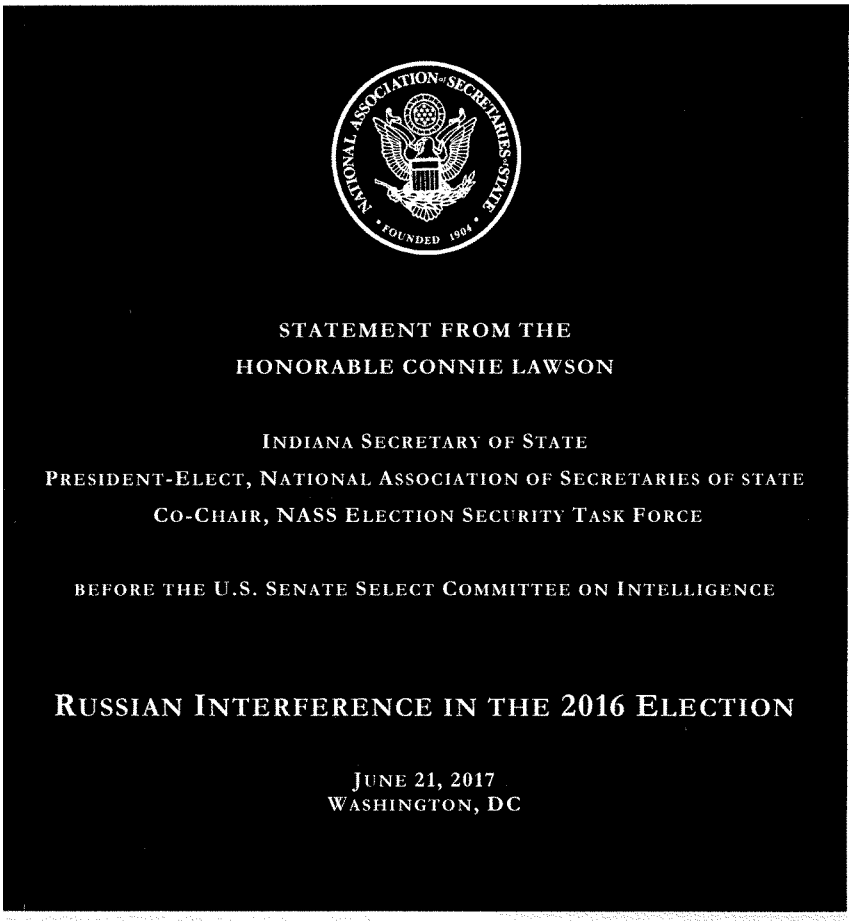
From information gaps to knowledge gaps that aren't being addressed, this process threatens to erode public confidence in the election process as much as any foreign cyber threat. It's also shredding the rights that states hold to determine their own election procedures subject to the acts of Congress. If the designation ultimately reduces diversity and autonomy in our voting process, the potential for adverse effects from perceived or real cyber effects—attacks excuse me—will likely be much greater and not the other way around.

Looking ahead, the National Association—the NASS Election Security Task Force was created to ensure that State election officials are working together to combat threats and foster effective partnerships with the Federal Government and other public-private stakeholders. In guarding against cyber threats, the trend line is positive, but more can be done. Most notably, many states and localities are working to replace or upgrade their voting equipment.

If I have one major request for you today, other than rescinding the critical infrastructure designation for elections, it is to help election officials get access to classified information-sharing. We need this information to defend State elections from foreign interference and respond to threats.

Thank you, and I look forward to answering your questions.

[The prepared statement of Ms. Lawson follows:]



STATEMENT FROM THE
HONORABLE CONNIE LAWSON

INDIANA SECRETARY OF STATE
PRESIDENT-ELECT, NATIONAL ASSOCIATION OF SECRETARIES OF STATE
CO-CHAIR, NASS ELECTION SECURITY TASK FORCE

BEFORE THE U.S. SENATE SELECT COMMITTEE ON INTELLIGENCE

RUSSIAN INTERFERENCE IN THE 2016 ELECTION

JUNE 21, 2017
WASHINGTON, DC

National Association of Secretaries of State
444 North Capitol Street, NW – Suite 401
Washington, DC 20001
202-624-3525 Phone
202-624-3527 Fax
www.nass.org

NASS
National Association of Secretaries of State

STATEMENT OF

HON. CONNIE LAWSON
INDIANA SECRETARY OF STATE
PRESIDENT-ELECT, NATIONAL ASSOCIATION OF SECRETARIES OF STATE
CO-CHAIR, NASS ELECTION SECURITY TASK FORCE

CONCERNING

RUSSIAN INTERFERENCE IN THE 2016 U.S. ELECTIONS

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

JUNE 21, 2017

Good morning, Chairman Burr, Vice Chairman Warner and distinguished Members of the Committee. Thank you for the chance to appear before you today to represent the nation's Secretaries of State, forty of whom serve as the chief state election official in their respective states. My name is Connie Lawson, and I am the Indiana Secretary of State. I am also president-elect of the bipartisan National Association of Secretaries of State (NASS), and in that leadership capacity, I also Co-Chair the NASS Election Security Task Force. NASS President Denise Merrill of Connecticut was not able to be here today, but I do want to acknowledge her outstanding leadership around the last election cycle and point out that we are a bipartisan organization.

It is an honor to be here with my distinguished fellow panelists to discuss what is ultimately our government's capacity to secure state and locally-run elections from Russian and other very significant and persistent nation-state cyberthreats. With statewide elections in New Jersey and Virginia this year, and many more contests to follow in 2018, I want to assure you – and all Americans – that election officials across the U.S. are taking cybersecurity very seriously. While it is important to ask what really happened in the 2016 cycle, we believe it is even more important for us to be discussing what lies ahead.

In this regard, we are struggling to understand – and implement – the U.S. Department of Homeland Security's January 2017 Executive Order designating elections as "critical infrastructure." I am part of the bipartisan majority of Secretaries of State who support a push to rescind the measure, which clashes with some of the most basic principles of our democracy and already seems likely to cause more problems than it actually solves. Furthermore, the time it has

taken to educate DHS on state and local elections, even after the designation was made, has been a drain on limited resources, which should be invested in strengthening election security.

I. FOREIGN TARGETING OF STATE AND LOCAL ELECTION SYSTEMS

First and foremost, I applaud you for holding this hearing today. This forum offers a chance to separate FACTS from FICTION regarding the 2016 presidential election.

As Senator Warner noted in a letter sent yesterday (June 20, 2017) to Homeland Security Secretary Kelly, we have not seen any credible evidence that vote casting or counting was subject to manipulation in any state or locality in the 2016 election cycle, or any reason to question the results. While still alarming, there is a big difference between manipulating VOTERS and manipulating VOTES.

Here is what chief state election officials know about documented foreign targeting of state and local election systems in the 2016 election cycle, as confirmed by DHS:

- No major cybersecurity issues were reported on Election Day: November 8, 2016. In certain areas of the nation where machine calibration or e-pollbook issues arose, they were immediately flagged to the attention of DHS.

- DHS confirmed to NASS that 33 states and 36 county jurisdictions had taken advantage of the agency's voluntary assistance by Election Day. NASS and DHS also achieved a joint goal of ensuring that all 50 states were notified of the federal government resources that were available to them upon request, including cyber hygiene scans on Internet-facing systems and risk and vulnerability assessments. Those states that did not utilize DHS assistance received similar support from their own state.

- We also learned that foreign-based hackers were able to gain access to voter registration systems in Arizona and Illinois last summer, prompting the Federal Bureau of Investigation (FBI) to warn state election offices to increase their election security measures for the November 2016 election. To our knowledge, no data was deleted or modified as part of the breaches, and these are not systems involved in vote tallying. A representative from the Illinois State Board of Elections is here to discuss that today, so I will let him speak to this subject.

- Of course, in more recent days, we have learned from a top-secret NSA report that the identity of a company providing voter registration support services in several states was compromised, and some 122 local election offices received spear phishing emails as a result. The vendor targeted by Russian military phishing emails operates in six Indiana counties, but here is where it is important to understand how elections work in many of the states.

> In Indiana, these six counties use this vendor's e-pollbook equipment, which is not connected to voting machines or tabulation machines.

While there is clearly a pattern of foreign targeting of election systems in the last cycle, it is also very important to underscore that voting machines are not connected to the Internet or networked in any way. I say this not only for the benefit of this Committee, but for the media as well. We must understand how to label, describe and discuss election infrastructure responsibly and accurately when informing the public about elections, because there has been a great deal of misinformation publicized, including statements from the federal government.

We have submitted for the record the Report on NASS Facts & Findings on Cybersecurity and Foreign Targeting of the 2016 U.S. Elections from March 2017.

It is gravely concerning that election officials have only recently learned about the threat referenced in the leaked NSA report, especially – and I emphasize this – given the fact that DHS repeatedly told state election officials no credible threat existed in the fall of 2016.

Secretaries of State took part in three calls where former DHS Secretary Jeh Johnson was asked whether any documented threats existed, on:

- August 15, 2016;
- September 8, 2016; and
- October 12, 2016.

Each time Secretary Johnson was directly asked about specific, credible threats and each time he confirmed that none existed.

We have submitted into the record a DHS readout of the first call that NASS had with Secretary Johnson after we proactively reached out to DHS and requested such a call. It remains unclear why our intelligence agencies would withhold timely and specific threat information from chief state election officials, who can use it to better defend their systems and neutralize specific threats.

I hope this Committee will be using its time to seek out the answer to this important question.

II. PROTECTING STATE AND LOCAL ELECTIONS FROM CYBER THREATS

Before I talk about ongoing cyber threats and the critical infrastructure designation for elections, I want to emphasize some of the systemic safeguards we have against cyber attackers. Our system is complex and decentralized, with a great deal of agility and low levels of connectivity. It is not a massive, centralized bureaucracy, but rather locally-run, bottom-up system.

Hon. Connie Lawson, Indiana Secretary of State
President-elect, NASS
Statement Before the U.S. Senate
June 21, 2017 | Washington, DC

NASS
National Association of Secretaries of State

As we repeatedly emphasized during the 2016 election cycle, diversity serves as a major check on the capabilities of nefarious actors to manipulate our voting process, because there is NO NATIONAL SYSTEM to target. Even within states, much diversity can exist from one locality to the next.

Researchers at Harvard University's Belfer Center noted in a 2016 report that for a federal election, manipulation at a level required to swing the result would be a significant undertaking. Their cybersecurity researchers noted that "for some methods of interference, manipulating 1,000 votes requires 1,000 times as much effort as manipulating one vote."[1]

While electoral interference can take many forms, including physical and cyber-based attacks, for the sake of today's hearing, I'll focus on three chief areas of concern to Secretaries of State:

- Attacks that target access to data or systems;
- Attacks that target their integrity; and
- Attacks that target their availability.

To my knowledge, we have only seen documented attacks of the first variety. Of course, that does not mean our adversaries won't try again. We are not naïve about the likelihood of future cyberattacks against digital elements of election systems.

I work with an excellent team, including Indiana's Information Sharing and Analysis Center (IN-ISAC). Indiana's Voting System Technical Oversight Program, run by Ball State University, requires all voting systems, tabulation systems and e-pollbooks to be certified prior to use. Indiana is developing more rigorous authentication processes.

I have every confidence that other panelists will address voting equipment risks and conceptual attack scenarios that are well-documented by academic researchers. Access control, data processing, cryptography and software design are important issues to be addressed moving ahead.

I would also caution that effective election administration is a constant balancing act between SECURITY and ACCESSIBILTY. Remember, our electoral process has been around for well over 200 years – long before the digital age. We can take down every electronic or online system we have, switch to paper ballots and hand counts and use only paper voter registration forms, but this type of security-first approach will result in a reduction to voter accessibility.

In some cases, the trade-offs may not be worthwhile. For example, finding that hackers accessed or copied voter file information is *by itself* not enormously significant—interested parties can often legally purchase voting roll information without hacking, as it's considered a matter of public record

[1] Ben Buchanan and Michael Sulmeyer. *Hacking Chads: The Motivations, Threats and Effects of Electoral Insecurity*, Harvard Kennedy School Belfer Center for Science and International Affairs, October 2016, pg. 12.

in most states. I don't want to get into discussing speculative "what if" scenarios here today, but I am happy to come back to this issue if you have any questions.

III. THE FUNDAMENTAL UNIQUENESS OF ELECTIONS AS CRITICAL INFRASTRUCTURE

This leads me to the Department of Homeland Security's designation of election systems as so-called "critical infrastructure" on January 6, 2017. It cannot be stressed enough: Elections are FUNDAMENTALLY DIFFERENT from any other sector or subsector of critical infrastructure.

At the outset, I want to appropriately describe the relationship between NASS and DHS. This winter, NASS adopted a bipartisan position opposing the designation. While some may find it inconsistent for NASS to collaborate with and educate DHS while working to have the designation rescinded, we must ensure the states have appropriate representation, regardless of the underlying position.

There is no question that expanded information-sharing between all levels of government will be helpful for increasing the resiliency of our electoral system.

Some additional issues that exist with the designation include:

- A lack of clear parameters around the order, which currently gives DHS and other federal agencies a large amount of unchecked executive authority over our elections process. At no time between August 2016 and January 2017 did NASS and its members ever have a thorough discussion or review of what the designation means (including questions answered) with DHS or anyone else at the federal level. In fact, my colleagues and I across the nation continued to ask for information at the time the designation was announced. We actually held a call with Secretary Johnson the day before, on January 5th, and the decision to move forward with the designation was never mentioned. Serious questions remain about the actual benefits of the designation, and the role of the other federal agencies as outlined in Presidential Policy Directive 21 (PPD-21), such as the Department of Justice, the Commerce Department, the General Services Agency and the U.S. Election Assistance Commission.

- According to PPD-21, which guides the federal government's approach, DHS – not the states – becomes the center of work to protect elections against independent and state-sponsored attacks – particularly cyberattacks. While election officials have been told their participation is "voluntary," it remains to be seen just how voluntary such commitments will be down the road. Will states be required to conform to new federal standards set forth with no real process or oversight in place? What resources or threat information will be withheld from states that do not voluntarily participate?

- There are also concerns about maintaining public trust in elections. U.S. government military and intelligence agencies can classify their work to shield it from public scrutiny. How will the broad exemptions from public records and sunshine laws that are afforded to critical infrastructure affect transparency in our electoral process? Right now, our system is designed to foster transparency and participation from end to end – from public testing of voting equipment to poll watchers to public counting of the ballots to post-election audits.

- Finally, Secretaries of State have serious concerns about the lack of federal government information-sharing regarding documented threats against election systems, particularly in the wake of the leaked NSA report. DHS touted threat-sharing as a key justification for the decision to designate elections as critical infrastructure. Yet, nearly six months after the designation and in spite of comments by DHS that they are rushing to establish their elections subsector, no Secretary of State is currently authorized to receive classified threat information from our intelligence agencies.

Think about that for a moment. If you are looking to improve election security, wouldn't you logically want to ensure that election officials are getting important information to help protect their systems? In fact, we have yet to hear any definitive statement by DHS on whether this designation will stand.

What is obvious is that setting up a hastily-formed subsector of critical infrastructure around elections isn't going to make us more secure. Thus far, there is a large knowledge gap that is unfortunately eroding confidence in the election process and shredding the rights that states hold to determine their own election procedures, subject to Acts of Congress. If the designation reduces diversity, autonomy and transparency in state and local election systems, the potential for adverse effects from perceived or real cyberattacks will likely be much GREATER – and not the other way around.

IV. PREPARING FOR THE 2018 CYCLE

I will conclude by briefly discussing preparations around upcoming elections, which as I mentioned are already underway.

The NASS Election Cybersecurity Task Force, which currently has members from 27 states, was created to ensure that state election officials are working together to combat threats and foster effective partnerships with the federal government and other public-private stakeholders. Some of the specific deliverables include:

- Developing resolutions on election cybersecurity to assist state election offices;

- Assisting NASS with guidance on federal government outreach and information-sharing related to election cybersecurity, including the DHS critical infrastructure designation for election infrastructure, assuming it will be retained under the President's administration;
- Developing and convening forums where new governance approaches and best practices can be discussed; and
- Sponsoring technical forums for those who are directly responsible for protecting digital election processes and systems.

We have already begun some important data collection to inform the work of the states. Additionally, we are also continuing our outreach to and education of DHS so the appropriate officials can receive classified information.

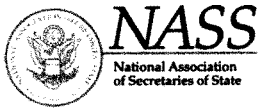
In the meantime, the DHS Inspector General is conducting an independent investigation into evidence of unauthorized scans that were performed from a DHS IP address against the Georgia Secretary of State's computer network. The Indiana Secretary of State's office has also submitted results of a state investigation that concluded with a "high degree of certainty" that similar unauthorized activity was detected against their computer network from the same IP address. Other states have similar concerns.

We need a forthright accounting from the Inspector General's office as soon as possible and hope to hear more on the status of this investigative work very soon.

In guarding against cyber threats, the trend line is positive, but more can be done. All but five states require their voting machines to produce a voter-verifiable paper trail that would enable recounts and audits, and we already know that some of those states are actively discussing their options. The majority of states have switched to optical scanning systems in which the voter marks a paper ballot that also serves as evidence for later verification.

Many states and localities are also working to upgrade their voting equipment. In 2016, 43 states used voting machines that are more than ten years old. Election officials have been approaching their state and county lawmakers about replacing or updating these systems to bolster their cybersecurity poster by 2018 or 2020.

In addition, the U.S. Election Assistance Commissions (EAC) Voluntary Voting System Guidelines (VVSGs) are being updated to reflect new ways to increase security and resiliency in voting machines and related technologies.



If I have one major request to Congress and the Administration other than rescinding the critical infrastructure designation for elections or placing clear parameters on the Executive Order, it would be to help election officials get access to classified information-sharing. We need this information to take appropriate actions to defend state elections from foreign interference and respond to threats.

According to a 2017 survey by the Center for Strategic and International Studies, fewer than half of respondent organizations are using unclassified government information as a source of information in making decisions about cybersecurity.[2] More than three-quarters believe that faster access to security clearances would be the most effective way to improve their cybersecurity posture, and 66% want greater access to threat intelligence. States see cooperation with our national intelligence agencies as an important part of their cybersecurity strategy, and with the right threat information-sharing info, an important part of increasing both the physical and the digital elements of their systems.

In conclusion, there is no doubt that more can – and WILL – be done to bolster resources, security protocols and technical support for state and local election officials heading into future elections. States continue to increase protection for their own systems, as evident by the already common trend of re-implementing handwritten ballots. With increased cooperation and diversity, and not expanded top-down regulation, elections systems will become more resilient and protected.

To quote a letter sent to election directors on September 28, 2016 by Senate Majority Leader McConnell, Senate Minority Leader Reid, House Majority Leader Ryan and House Minority Leader Pelosi:

"The local authorities who bear the responsibility cannot now, and should not in the future be able to, point the finger of blame at some distant, unaccountable, centralized bureaucracy.... For over 200 years states have overcome every challenge to ensure the smooth functioning of our democracy. We trust now that you will take the steps necessary to meet the challenges of the 21st century by securing your election systems against cyberattacks."

I want to thank the Committee again for holding this hearing and for giving me the opportunity to speak about this important matter on behalf of NASS. I look forward to answering any questions you may have for me.

Thank you.

[2] *Tilting the Playing Field: How Misaligned Incentives Work Against Cybersecurity*, Center for Strategic and International Studies, February 2017, pg. 17.

Chairman BURR. Thank you, Secretary Lawson.

Who would like to—Mr. Haas.

STATEMENT OF MICHAEL HAAS, MIDWEST REGIONAL REPRESENTATIVE, NATIONAL ASSOCIATION OF STATE ELECTION DIRECTORS

Mr. HAAS. Thank you. Good morning.

Chairman Burr, Vice Chairman Warner and Committee members: On behalf of the National Association of State Election Directors, thank you for this opportunity to share what states learned from the 2016 elections and some steps that we are taking to further secure our election systems.

I serve as Wisconsin's chief election official, and I'm a member of NASED's executive board. We do not have a State elected official who oversees elections in Wisconsin. Many of our State election directors across the country are housed in the secretary of state's offices, but some are not.

The 2016 presidential election reinforced several basic lessons, although sometimes in a new context. For instance, all of us understand the importance of constant and effective communication to ensure that all actors have the tools they need. The new twist in 2016, of course, involved communicating about the security of election systems with the Department of Homeland Security as well as the State staff who provide cyber security protection to our voter registration databases.

As we have heard this morning, some states have expressed concerns about the timeliness and the details of communications from Homeland Security regarding potential threats, security threats to State election systems. The recent reports about attempted attacks on State voter registration systems, which occurred last fall, caught many states by surprise.

We look forward to working with DHS and other Federal officials to develop protocols and expectations for communicating similar information going forward. For example, State election officials believe it is important that we be in the loop regarding contacts that DHS has with local election officials regarding security threats such as the spear phishing attempts that were recently publicized. States should be aware of this information to protect their systems and so that we can provide additional training and guidance to local election officials.

I appreciate the concern that was expressed this morning that this is a two-way street. And we at the State level need to also think carefully about how to most effectively communicate with our local election officials if and when there is an incident that we are aware of at the State level.

As part of the DHS designation of election systems as critical infrastructure, bodies such as coordinating councils can help to facilitate decisions regarding the proper balance between notifying State and local officials and protecting confidential or sensitive information.

NASED believes that those coordinating bodies should consist of a broad representation of stakeholders, and we have expressed our strong interest to DHS in participating on those bodies.

I would also note that the executive board of NASED supports the request of the U.S. Elections Assistance Commission that it serves as the co-sector specific—specific agency as the logical Federal agency to partner with DHS to provide subject matter expertise and assistance in communicating with local election officials, as the EAC has that communications structure already in place.

The 2016 elections also reinforced the need for constantly enhancing the security of voter registration databases, as we have heard this morning. While hacking into a voter registration system has no effect on tabulating election results, intrusions could result in unauthorized parties gaining access to data regarding voters, candidates, ballot contests, and polling places.

I would note that, while much of that information is public upon request, there may be some confidential data held in those databases, such as the voter's date of birth, the driver license number, the last four digits of the social security number. Different states have different laws about what pieces of that data are confidential.

The 2016 elections demonstrated that State and local election officials can implement steps to improve the security of voter data, and that many of these steps are not complicated. In addition to the cyber hygiene scans and risk assessments, states are implementing greater use of multi-factor authentication for users of our systems, updating firewalls, the use of white lists to block unauthorized users, and completely blocking access from any foreign IP address.

The final lesson of 2016 I would like to address relates to voting equipment. To be clear, as it has been said many times this morning, there is no evidence that voting machines or election results have been altered in U.S. elections. I appreciate the Committee's emphasis on that. I think that for the public that cannot be stated enough and strongly enough.

Still, we as election administrators must exercise vigilance to assure that such theoretical attacks do not become reality, and we must also continue to educate the public about safeguards in the system. Those safeguards include the decentralized structure of elections that we've heard about this morning and the diversity of voting equipment. Also, in most cases voting equipment is not connected to the Internet and therefore cannot be attacked through cyber space. Also it is important to keep in mind that three out of four ballots cast in American elections are on paper ballots. Most ballots cast on touchscreen equipment also have a paper trail that voters can immediately verify their votes and that election officials can use for audits and recounts.

There are also several redundancies in the testing and certification of voting equipment. It's important to realize that voting equipment is not only used on Election Day. Its functionality is tested several times during the process.

In short, the 2016 elections taught us that the potential for disrupting election processes and technology by foreign or domestic actors is a serious and increasing concern. However, we as State election directors believe that continued cooperation and more effective communication, along with continued vigilance and innovation, will ensure the integrity of our voting processes and election results.

Again, we look forward to working with our Federal partners as we plan for elections going forward. Thank you for the opportunity to share these thoughts and I'd be happy to answer any questions.

[The prepared statement of Mr. Haas follows:]

Testimony of Michael Haas
Administrator
Wisconsin Elections Commission

United States Senate Select Committee on Intelligence
June 21, 2017

Elections Security:
Lessons Learned and Continued Vigilance

Chairman Burr, Ranking Committee Member Warner and Committee Members:

Thank you for the opportunity to provide information to the Senate Select Committee on Intelligence about what states learned from the 2016 elections and some steps that states are taking to secure elections systems as we prepare for future elections. I am honored to provide some thoughts on behalf of the National Association of State Election Directors (NASED) and our President, Judd Choate, the state elections director of the State of Colorado, who is unable to be here today due to family commitments. I am a member of NASED's Executive Board as its Midwest Region Representative.

Diversity of State Election Administration Systems

Before discussing the security of voter registration databases and voting equipment, it may be helpful to provide some brief background about the differences in election administration among the states, which is a true reflection of our federal system. In many states, the elected Secretary of State is designated as the state's chief election official, while the Lieutenant Governor serves that role in a handful of states. The state may have an elections director who is part of those offices and/or an elections board. Wisconsin has a unique structure with a bipartisan Elections Commission made up of three Republican appointees and three Democratic appointees, which oversees the agency and which appointed me as the agency's nonpartisan administrator and the state's chief election official.

At the state level, chief election officials and staffs are responsible for administering and enforcing election laws and procedures. This includes maintaining the statewide voter registration database as required by federal law, approving and sometimes purchasing voting equipment used in the state, training local election officials and poll workers, collecting and certifying official election results, and providing information to voters. In most states, elections are actually conducted by county clerks or registrars. Eight states, including Massachusetts and Michigan, conduct elections at the local level. In Wisconsin, we have 1,853 municipal clerks who conduct elections. As in other states, our agency is responsible for training each of those clerks so that election laws and voting procedures are administered properly and consistently throughout the state.

Finally, there are differences among the states in how voting and voter registration is conducted and in the ways that technology solutions are used. Some states maintain their voter registration database in-house and others rely on vendors. In recent years, states have developed and implemented various tools such as online voter registration, universal or automatic registration, electronic poll books, electronic transmission of blank ballots to absentee voters, and cross-state sharing of voter data in different combinations and on their own timetables. Some states use vote centers rather than traditional neighborhood polling places. Three states – Oregon, Washington and Colorado – hold elections entirely by mail.

These variations among the states illustrate different approaches but the same basic goals – to ensure the right to vote of every qualified elector, ensure the security of election systems and processes, maintain current and accurate voter lists, accommodate evolving trends in voter behavior, and reduce opportunities for administrative or human error. Ultimately, the common goal of election officials is to obtain the most accurate count of the vote so that candidates, voters and the public will have the utmost confidence in the integrity of our elections.

Regardless of the particular structure and tools of election administration among the states, several basic lessons were reinforced in the 2016 elections, although sometimes in a new context.

Effective Communication

First is the importance of constant, timely and effective communication with all of our partners so that all actors in the system have the tools they need. For example, the Elections Assistance Commission (EAC) develops many guides and other resources for election officials. NASED and other organizations such as the Election Center and the Election Academy provide professional education, training and tools.

At the state level we must communicate effectively with both federal agencies and local election officials. A simple example of this was the U.S. Postal Service's change in mail delivery standards. Last year the Postal Service advised that voters mailing in an absentee ballot do so at least a week before Election Day, even though many state laws establish a later deadline for voters to request absentee ballots. State election officials needed to communicate this change in policy to voters and encouraged local clerks to do the same.

The new twist in 2016 was the importance of communications regarding the security of election systems and equipment, specifically with the Department of Homeland Security and with the entities which provide cybersecurity protection to our voter registration databases. More than 30 states accepted DHS's offers of assistance leading up to the Presidential Election, including cyber hygiene scans of voter registration systems and other election technology, and risk and vulnerability assessments and recommendations. This assistance supplemented steps taken by state election offices and their respective

state IT agencies to monitor activity related to these systems and regularly consult regarding the status of those systems as well as security measures being implemented. States also increased cooperative efforts with the FBI and U.S. Attorneys, as well as state-level emergency management agencies.

In recent years many state election agencies have spent significant time educating state chief information officers and their staffs regarding the interaction of election processes with state IT infrastructure. A similar effort has taken place with the Department of Homeland Security since its emergence as a key partner in elections administration last summer. I believe DHS would acknowledge that its understanding of election administration was somewhat rudimentary when it entered this area last summer. Through communicating with secretaries of state and state election directors, its expertise regarding elections and appreciation for our concerns has improved but more can be done in this regard.

DHS would also readily acknowledge that some of its state partners have expressed concerns about the timeliness and the details of its communications regarding election security and potential threats to state systems. The recent reports about attempted attacks on state voter registration systems, which occurred last fall, caught many states by surprise. There is, of course, a balance needed between sharing information with those who may be affected and can take steps to address vulnerabilities and the need to maintain the confidentiality of information that is either classified or may have important law enforcement or national security ramifications.

State election officials understand that ongoing tension and look forward to working with DHS and other federal officials to develop protocols and expectations for communicating that type of information going forward. For example, state election officials believe it is important that they be in the loop regarding contacts that DHS has with local election officials regarding security threats such as the spear-phishing attempts that were recently publicized. After all, those attacks threatened state databases by attempting to gain access through a vendor and local election officials. States need to be aware of this information to protect their systems and so that we can provide additional training and guidance to local election officials.

As part of the DHS designation of election systems as critical infrastructure, bodies such as Coordinating Councils and Information Sharing and Analysis Centers can help to facilitate those discussions and decisions. NASED agrees with DHS that those bodies should consist of a broad representation of stakeholders.

I have provided to the Committee a copy of a letter from NASED President Judd Choate to DHS expressing our strong interest in participating on those bodies, and in forming them as soon as possible. State election officials are already in the midst of planning for 2018 elections and a fully functioning Elections Coordinating Council is important to the success of those efforts.

I would also note that the EAC has requested that DHS designate it as the Co-Sector Specific Agency at the federal level to provide subject matter expertise, resources and assistance in coordinating communications with state and local election officials. While the NASED membership has not taken a formal vote regarding the designation of the EAC as the federal Co-Sector Specific Agency, the NASED Executive Board endorses that request of the EAC.

Securing Voter Registration Databases

In addition to the importance of effective communication with our partners, the 2016 elections reinforced the need for constantly enhancing the security of voter registration databases. As DHS and election officials have tried to clarify, hacking into a voter registration system has no effect on the counting of ballots or tabulating election results. Voter registration systems contain data regarding voters, candidates, ballot contests, and polling places. If not prevented, intrusions could result in unauthorized parties gaining access to that information.

IT experts will note that no system is 100 percent secure from hacking. However, there is much that state and local election officials can do to improve the security of voter data. The 2016 elections demonstrated that many of these steps are not complicated, and the good news is that states are working to implement steps that will help detect and prevent hacking attempts in the future. In addition to the cyber hygiene scans completed by DHS and state IT agencies, some of those steps include greater use of multi-factor authentication for users of our systems, installing updated firewalls, the use of whitelists to block individuals using unauthorized email addresses or domain names from accessing the system, and completely blocking access from any foreign IP address.

Recently, David Becker, Executive Director of the Center for Election Innovation and Research, posted a helpful blog which placed reports of election system hacking into their proper context and recommended several additional steps for states going forward. These include conducting an analysis of voter registration activity in the days leading up to an election and comparing it to activity prior to past elections. For instance, queries may be completed to detect when multiple absentee ballots are requested for the same address, or to give additional scrutiny to requests that absentee ballots be sent to addresses out of the state and out of the country. Such queries may be an additional tool to ensure that only qualified and registered electors are receiving ballots.

Finally, states continue to improve their voter list maintenance practices by implementing more accurate and current data matching processes, with partner agencies both from the same state and across states. After a decade of experience matching data of individuals contained in the voter registration system with records from motor vehicle agencies and death records, some states are revamping their voter registration systems and rethinking those data matching processes. Keeping the voter registration lists accurate and up-to-date is a basic but crucial exercise which leads to efficiencies throughout the election process and minimizes opportunities for the misuse of outdated voter records.

Many jurisdictions are also participating in cooperative data sharing efforts across state lines. Wisconsin is one of 22 states and the District of Columbia which are members of the Electronic Registration Information Center (ERIC), which conducts comparisons of voter records from member states to identify individuals who may be registered in more than one state, or who may have moved within or between member states. More than 30 states participate in the Interstate Voter Registration Crosscheck Program, which attempts to identify individuals who have either registered or voted in more than one state.

In both cases, election officials may take steps to confirm the change in the voter's status and update records accordingly. What we have learned is that a possible computer match is not necessarily the same thing as an actual match involving the same individual, and the eyes of trained local election officials are still required to weed out real matches from the false positive matches.

Securing Voting Equipment

The final lesson of 2016 I would like to address relates to voting equipment. It is no secret that some jurisdictions throughout the country face challenges in funding the purchase of voting equipment to replace aging equipment which operates with older technology. In some cases, replacement parts are difficult to locate and vendors are discontinuing maintenance of the equipment. This remains a significant challenge which will continue to receive the attention of state and local election officials.

While not new, claims persisted in 2016 that voting equipment could be easily hacked and results could be altered. In the past, such claims were ostensibly supported by videotaped demonstrations of individuals who had physical access to individual voting machines and who installed malware into the tabulating software which counts the ballots. This represented an unlikely scenario in the real world given the processes used to program, test and secure voting equipment and programming software.

More recently, some have asserted that voting equipment can be attacked with malicious software remotely, through the election management software that programs equipment to count individual contests on the ballot and that is installed on individual voting machines.

To be clear, there has not been any evidence that voting machines or election results have been altered in U.S. elections. Still, election administrators must exercise vigilance to assure that such theoretical attacks do not become a reality. In order to maintain public confidence in election results, we must also continue to educate the public about safeguards in the system which help to prevent unauthorized access to and altering of voting equipment. These safeguards include the following:

- The decentralized structure of American elections means that multiple types of voting equipment are used across the country and often within individual states.

The diversity of equipment used and elections conducted at the local level help to create obstacles to large scale, coordinated attacks on voting equipment.

- In most cases, voting equipment is not connected to the Internet and therefore it cannot be attacked through cyberspace. When voting results are transmitted electronically on Election Night, it is after the polls are closed, the results are still unofficial, and they are transmitted using a cellular network rather than over the Internet.

- Approximately three-quarters of ballots cast in American elections are paper ballots, and most ballots cast on touch screen equipment result in a paper trail that can be immediately verified by the voter as well as by election officials through a recount or audit of the voting equipment.

- States implement overlapping and redundant processes to monitor and test the performance of voting equipment. Many states rely on the federal testing and certification program of the EAC and/or conduct their own testing and approval process before equipment may be used in the state. Public tests of voting equipment are conducted prior to each election and equipment is physically secured when it is not in use in an election. Finally, many states conduct post-election audits of voting equipment to ensure that votes are counted accurately as required under state law. As a result, Election Day is not the only time that voting equipment and its technology is under scrutiny.

Conclusion

In summary, I would reiterate that the American election system is characterized by decentralization, multi-faceted partnerships among federal, state and local officials, and constant innovations in the use of technology, data and best practices. The potential for disrupting election processes and technology by foreign or domestic actors is a serious and increasing concern. That lesson was clear in 2016 and continues to be a reality.

I believe I can state with confidence, however, the view of state election directors. Continued cooperation among those in the elections profession and in law enforcement, along with continued vigilance and innovation, will ensure the integrity of our voting processes and election results. We look forward to working with our federal partners as we plan for a full calendar of elections in 2018.

Thank you for the opportunity to share my thoughts with you. I would be happy to answer any questions that Committee Members may have.

Chairman BURR. Thank you, Mr. Haas.
Mr. Sandvoss.

STATEMENT OF STEVE SANDVOSS, EXECUTIVE DIRECTOR OF ILLINOIS STATE BOARD OF ELECTIONS

Mr. SANDVOSS. Good morning. Thank you, Chairman Burr, Vice Chairman Warner, and distinguished members of the Committee.

As Director of the State Board of Elections, I'd just like to briefly describe what our agency does. We are an independent bipartisan agency created by the 1970 Illinois Constitution, charged with general supervision over the election and registration laws in the State of Illinois.

As all of you seem to be aware, almost a year ago today, on June 23rd, the Illinois State Board of Elections was the victim of a malicious cyber attack of unknown origin against the Illinois voter registration system database. Because of the initial low-volume nature of the attack, the State Board of Elections staff did not become aware of it at first.

Almost three weeks later, on July 12th, State Board of Elections IT staff was made aware of performance issues with the IVRS database server. The processor's usage had spiked to 100 percent with no explanation. Analysis of the server logs revealed that the heavy load was a result of rapidly repeated database queries on the application status page of our paperless online voter application website.

Additionally, the server log showed the database queries were malicious in nature. It was a form of cyber attack known as SQL, which is "structured query language injection." SQL injections are essentially unauthorized malicious database queries entered into a data field in a web-based application. We later determined that these SQLs originated from several foreign-based IP addresses.

SBE programmers immediately introduced code changes to eliminate this particular vulnerability in our website. The following day, on July 13th, the SBE IT made the decision to take the website and IVRS database offline to investigate the severity of the attack. SBE staff maintained the ability to log and view all site access attempts.

Malicious traffic from the IP addresses continued, though it was blocked at the firewall level. Firewall monitoring indicated that the attackers were hitting SBE IP addresses five times per second, 24 hours a day. These attacks continued until August 12th, when they abruptly ceased.

SBE staff began working to determine the extent of the breech, analyzing the integrity of the IVRS database and introducing security enhancements to the IVRS web servers and database.

A week later, on July 19th, we notified the Illinois General Assembly of the security breech in accordance with the Personal Information Protection Act. In addition, we notified the Attorney General's office. On July 21st, the State Board of Elections' IT staff completed security enhancements and began to bring the IVRS system back on line. A week after that, on July 28th, both the Illinois registration system and the paperless online voting application became totally functional once again.

Since the attack occurred, the State Board of Elections has maintained the following ongoing activities. The DHS scans the State Board of Elections systems for vulnerabilities on a weekly basis. The Illinois Department of Innovation and Technology, which is a statewide entity that coordinates the IT systems of many of the Illinois State agencies, continuously monitors activity on the Illinois Century Network, which is the general network that provides firewall protection for the State computer systems.

This Department of Innovation and Technology, also called DOIT, provided cyber security awareness training for all State of Illinois employees, ours included. Now the State Board of Election's IT staff continues to monitor web server and firewall logs on a daily basis. And in addition, virus protection software is downloaded also on a daily basis.

As a result of informing the Illinois Attorney General's office of the breach, the State Board of Elections was contacted by the Federal Bureau of Investigation, and we have fully cooperated with the FBI in their ongoing investigation. The FBI advised that we work with the Department of Homeland Security's United States Computer Emergency Readiness Team to ensure that there is no ongoing malicious activity on any of the SBE systems. They also confirmed—that is, the Department of Homeland Security also confirmed—that there's no ongoing malicious activity occurring in SBE computer systems.

To comply with the Personal Information Protection Act, nearly 76,000 registered voters were contacted as potential victims of the data breach. The SBE provided information to these individuals on steps to take if they felt that they were the victims of identity theft. Additionally, the SBE developed an online tool to inform affected individuals of the specific information that was included in their voter record that may have been compromised.

As far as looking for future concerns, one of the concerns facing our State and many others we believe is aging voting equipment. The Help America Vote Act established requirements for voting equipment, but while initial funding was made available to replace the old punch-card equipment, additional funding has not been further appropriated.

If additional funding is not available, we would like to receive authorization to use the State's existing HAVA funds to allow spending on enhanced security across all election-related systems. The IVRS database is a Federal mandate through the Help America Vote Act.

Cyber attacks targeting end users are also of particular concern. Security training funded and provided by a Federal entity such as the EAC or DHS would also be beneficial in our view. In addition, any guidance or recommendations as to methods for the protection of registration and voting systems from cyber intrusions are always welcome.

Thank you for the time, and I'm happy to answer any questions.

[The prepared statement of Mr. Sandvoss follows:]

Illinois Voter Registration System Database Breach Report

The Illinois State Board of Elections was the victim of a malicious cyber-attack of unknown origin against the Illinois Voter Registration System database (IVRS) beginning June 23, 2016. Because of the initial low volume nature of the attack, SBE staff did not become aware of the breach until the volume dramatically increased on July 12th. At that point, SBE IT immediately took measures to stop the intrusion. In the following weeks, SBE staff worked to determine the scope of the intrusion, secure databases and web applications, comply with state law regarding personal information loss, and assist law enforcement in their investigation of the attack.

Analysis concluded that in addition to viewing multiple database tables, attackers accessed approximately 90,000 voter registration records.

Timeline

July 12, 2016

State Board of Elections IT staff was made aware of performance issues with the IVRS database server. Processor usage had spiked to 100% with no explanation. Analysis of server logs revealed that the heavy load was a result of rapidly repeated database queries on the application status page of the Paperless Online Voter Application (POVA) web site. Additionally, the server logs showed the database queries were malicious in nature – a form of cyber-attack known as SQL (Structured Query Language) Injection. SQL Injections are essentially unauthorized, malicious database queries entered in a data field in a web based application. We later determined that these SQLs originated from several foreign based IP addresses.

SBE programmers immediately introduced code changes to eliminate this vulnerability.

July 13, 2016

SBE IT took the web site and IVRS database offline to investigate the severity of the attack.

Analysis of the web server logs showed that malicious SQL queries had begun on June 23, 2016.

SBE staff maintained the ability to log and view all site access attempts. Malicious traffic from the IP addresses continued, though it was blocked at the firewall level. Firewall monitoring indicated that the attackers were hitting SBE IP addresses 5 times per second, 24 hours per day.

SBE staff began working to determine the extent of the breach, analyzing the integrity of the IVRS database, and introducing security enhancements to the IVRS web servers and database.

July 19, 2016

We notified the Illinois General Assembly of the security breach in accordance with the Personal Information Protection Act (PIPA). In addition, we notified the Illinois Attorney General's office.

July 21, 2016

SBE IT completed security enhancements and began bringing IVRS back online.

July 28, 2016

Both the Illinois Voter Registration System and the Paperless Online Voter application became fully functional.

Ongoing

SBE IT staff continues to monitor its web server and firewall logs on a daily basis.

Outside Agency Participation

As a result of informing the Illinois Attorney General's office of the breach, the SBE was contacted by the Federal Bureau of Investigation. We have fully cooperated with the FBI in their ongoing investigation.

The Illinois Department of Innovation and Technology (which is a State-wide entity that coordinates the IT systems of the various State agencies) was helpful by providing web traffic logs and assisting with web server log analysis.

The FBI advised that we work with the Department of Homeland Security's (DHS) United States Computer Emergency Readiness Team (US-CERT) to ensure there was no ongoing malicious activity on any of SBE's systems.

PIPA Compliance

Nearly 76,000 registered voters were contacted as potential victims of the data breach.

The SBE provided these individuals information on steps to take if they felt they were the victims of identity theft. Additionally, the SBE developed an online tool to inform affected individuals of the specific information included in their voter record.

Future Concerns

Voting Equipment – One of the concerns facing our state and many others is aging voting equipment. The Help America Vote Act (HAVA) established requirements for voting equipment, but, while initial funding was made available, additional funding has not been appropriated.

In addition to future funding, HAVA restrictions on spending could be relaxed to allow spending on enhanced security across all election-related systems.

New Standards for Voting Equipment

Security Training and Guidance for State and Local Election Officials – Cyberattacks targeting end users are of particular concern. Security training funded and provided by a federal entity such as the EAC would be beneficial. In addition, any guidance or recommendations as to methods for the protection of registration and voting systems from cyber intrusions are always welcome.

Chairman BURR. Thank you, Mr. Sandvoss.
Dr. Halderman.

STATEMENT OF J. ALEX HALDERMAN, Ph.D., PROFESSOR OF COMPUTER SCIENCE AND ENGINEERING, UNIVERSITY OF MICHIGAN

Dr. HALDERMAN. Chairman Burr, Vice Chairman Warner, and members of the Committee: Thank you for inviting me to speak with you today about the security of U.S. elections.

I'm a Professor of Computer Science and have spent the last 10 years studying the electronic voting systems that our Nation relies on. My conclusion from that work is that our highly computerized election infrastructure is vulnerable to sabotage and even to cyber attacks that could change votes. These realities risk making our election results more difficult for the American people to trust.

I know America's voting machines are vulnerable because my colleagues and I have hacked them repeatedly as part of a decade of research studying the technology that operates elections and learning how to make it stronger. We've created attacks that can spread from machine to machine, like a computer virus, and silently change election outcomes. We've studied touchscreen and optical scan systems, and in every single case we found ways for attackers to sabotage machines and to steal votes. These capabilities are certainly within reach for America's enemies.

As you know, states choose their own voting technology and, while some states are doing well with security, others are alarmingly vulnerable. This puts the entire Nation at risk. In close elections, an attacker can probe the most important swing states or swing counties, find areas with the weakest protection, and strike there. In a close election year, changing a few votes in key localities could be enough to tip national results.

The key lesson from 2016 is that these threats are real. We've heard that Russian efforts to target voter registration systems struck 21 states, and we've seen reports detailing efforts to spread an attack from an election technology vendor to local election offices. Attacking vendors and municipalities could have put Russia in a position to sabotage equipment on Election Day, causing machines or poll books to fail, and causing long lines or disruption. They could have engineered this chaos to have a partisan effect by striking places that lean heavily towards one candidate.

Some say the fact that voting machines aren't directly connected to the Internet makes them secure, but unfortunately, this is not true. Voting machines are not as distant from the Internet as they may seem. Before every election, they need to be programmed with races and candidates. That programming is created on a desktop computer, then transferred to voting machines. If Russia infiltrated these election management computers, it could have spread a vote-stealing attack to vast numbers of machines.

I don't know how far Russia got or whether they managed to interfere with equipment on Election Day, but there's no doubt that Russia has the technical ability to commit widespread attacks against our voting system, as do other hostile nations. I agree with James Comey when he warned here two weeks ago: We know

they're coming after America, and they'll be back. We must start preparing now.

Fortunately, there's a broad consensus among cybersecurity experts about measures that would make America's election infrastructure much harder to attack. I've co-signed a letter that I've entered into the record from over 100 leading computer scientists, security experts, and election officials that recommends three essential steps.

First, we need to upgrade obsolete and vulnerable voting machines, such as paperless touchscreens, and replace them with optical scanners that count paper ballots. This is a technology that 36 states already use. Paper provides a physical record of the vote that simply can't be hacked.

President Trump made this point well on Fox News the morning after—the morning of the election. He said, "There's something really nice about the old paper ballot system. You don't worry about hacking."

Second, we need to use the paper to make sure that the computer results are right. This is a common-sense quality control and it should be routine. Using what's known as a risk-limiting audit, officials can check a small, random sample of the ballots to quickly and affordably provide high assurance that the election outcome was correct. Only two states, Colorado and New Mexico, currently conduct audits that are robust enough to reliably detect cyber attacks.

Lastly, we need to harden our systems against sabotage and raise the bar for attacks of all sorts by conducting comprehensive threat assessments and applying cybersecurity best practices to the design of voting equipment and the management of elections.

These are affordable fixes. Replacing insecure paperless voting machines nationwide would cost $130 million to $400 million. Running risk-limiting audits nationally for Federal elections would cost less than $20 million a year. These amounts are vanishingly small compared to the national security improvement they buy.

State and local election officials have an extremely difficult job, even without having to worry about cyber attacks by hostile governments. But the Federal Government can make prudent investments to help them secure elections and uphold voters' confidence. We all want election results that we can trust.

If Congress works closely with the states, we can upgrade our election infrastructure in time for 2018 and 2020. But if we fail to act, I think it's only a matter of time until a major election is disrupted or stolen in a cyber attack.

Thank you for the opportunity to testify today and for your leadership on this critical matter. I look forward to answering any questions.

[The prepared statement of Dr. Halderman follows:]

U.S. Senate Select Committee on Intelligence

Russian Interference in the 2016 U.S. Elections

Expert Testimony by
J. Alex Halderman
Professor of Computer Science, University of Michigan

June 21, 2017

Chairman Burr, Vice Chairman Warner, and members of the Committee, thank you for inviting me to speak today about the security of U.S. elections. I'm here to tell you not just what I think, but about concerns shared by hundreds of experts from across cybersecurity research and industry. Such expertise is relevant because elections—the bedrock of our democracy—are now on the front lines of cybersecurity, and they face increasingly serious threats. Our interest in this matter is decidedly non-partisan; our focus is on the integrity of the democratic process, and the ability of the voting system to record, tabulate, and report the results of elections accurately.

My research in computer science and cybersecurity tackles a broad range of security challenges.[1] I study attacks and defenses for the Internet protocols we all rely on every day to keep our personal and financial information safe. I also study the capabilities and limitations of the world's most powerful attackers, including sophisticated criminal gangs and hostile nation states. A large part of my work over the last ten years has been studying the computer technology that our election system relies on.[2] In this work, I often lead the "red team," playing the role of a potential attacker to find where systems and practices are vulnerable and learn how to make them stronger.

I know firsthand how easy it can be to manipulate computerized voting machines. As part of security testing, I've performed attacks on widely used voting machines, and I've had students successfully attack machines under my supervision.

---

[1] My curriculum vitae and research publications are available online at https://jhalderm.com.
[2] For an accessible introduction to the security risks and future potential of computer voting technologies, see my online course, *Securing Digital Democracy*, which is available for free on Coursera: https://www.coursera.org/learn/digital-democracy.

U.S. Voting Machines Are Vulnerable

As you know, states choose their own voting technology.[3] Today, the vast majority of votes are cast using one of two computerized methods. Most states and most voters use the first type, called optical scan ballots, in which the voter fills out a paper ballot that is then scanned and counted by a computer. The other widely used approach has voters interact directly with a computer, rather than marking a choice on paper. It's called DRE, or direct-recording electronic, voting. With DRE voting machines, the primary records of the vote are stored in computer memory.[4]

Both optical scanners and DRE voting machines are computers. Under the hood, they're not so different from your laptop or smartphone, although they tend to use much older technology—sometimes decades out of date.[5] Fundamentally, they suffer from security weaknesses similar to those of other computer devices. I know because I've developed ways to attack many of them myself as part of my research into election security threats.

Ten years ago, I was part of the first academic team to conduct a comprehensive security analysis of a DRE voting machine. We examined what was at that time the most widely used touch-screen DRE in the country,[6] and spent several months probing it for vulnerabilities. What we found was disturbing: we could reprogram the machine to invisibly cause any candidate to win. We also created malicious software—vote-stealing

---

[3] In many states, the technology in use even differs from county to county. Verified Voting maintains an online database of the equipment in use in each locality: https://www.verifiedvoting.org/verifier/.

[4] Some DREs also produce a printed record of the vote and show it briefly to the voter, using a mechanism called a voter-verifiable paper audit trail, or VVPAT. While VVPAT records provide a physical record of the vote that is a valuable safeguard against cyberattacks, research has shown that VVPAT records are difficult to accurately audit and that voters often fail to notice if the printed record doesn't match their votes. For these reasons, most election security experts favor optical scan paper ballots. See: S. Goggin and M. Byrne, "An Examination of the Auditability of Voter Verified Paper Audit Trail (VVPAT) Ballots." In *Proceedings of the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop*, August 2007. Available at: http://www.accurate-voting.org/wp-content/uploads/2007/08/evt07-goggin.pdf. See also: B. Campbell and M. Byrne, "Now Do Voters Notice Review Screen Anomalies?" In *Proceedings of the 2009 USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop*, August 2009. Available at: http://chil.rice.edu/research/pdf/CampbellByrne_EVT_(2009).pdf.

[5] In 2016, 43 states used computer voting machines that were at least 10 years old—close to the end of their design lifespans. Older hardware and software generally lacks defenses that guard against more modern attack techniques. See: L. Norden and C. Famighetti, "America's Voting Machines at Risk," Brennan Center, 2015. https://www.brennancenter.org/publication/americas-voting-machines-risk. See also: S. Checkoway, A. Feldman, B. Kantor, J. A. Halderman, E. W. Felten, and H. Shacham, "Can DREs Provide Long-Lasting Security? The Case of Return-Oriented Programming and the AVC Advantage." In *Proceedings of the 2009 USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop*, August 2009. Available at: https://jhalderm.com/pub/papers/avc-evt09.pdf.

[6] The machine was the Diebold AccuVote TS, which is still used statewide in Georgia in 2017.

code—that could spread from machine-to-machine like a computer virus, and silently change the election outcome.[7]

Vulnerabilities like these are endemic throughout our election system. Cybersecurity experts have studied a wide range of U.S. voting machines—including both DREs and optical scanners—and in *every single case,* they've found severe vulnerabilities that would allow attackers to sabotage machines and to alter votes.[8] That's why there is overwhelming consensus in the cybersecurity and election integrity research communities that our elections are at risk.

Cyberattacks Could Compromise Elections

Of course, interfering in a state or national election is a bigger job than just attacking a single machine. Some say the decentralized nature of the U.S. voting system and the fact that voting machines aren't directly connected to the Internet make changing a state or national election outcome impossible. Unfortunately, that is not true.[9]

Some election functions are actually quite centralized. A small number of election technology vendors and support contractors service the systems used by many local governments. Attackers could target one or a few of these companies and spread malicious code to election equipment that serves millions of voters.

Furthermore, in close elections, decentralization can actually work against us. An attacker can probe different areas of the most important "swing states" for vulnerabilities, find the areas that have the weakest protection, and strike there.[10] In a close election, changing a few votes may be enough to tip the result, and an attacker can choose where—and on which equipment—to steal those votes. State and local elections are also at risk.

---

[7] A. J. Feldman, J. A. Halderman, and E. W. Felten, "Security Analysis of the Diebold AccuVote-TS Voting Machine." In *Proceedings of the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop* (EVT), August 2007. The research paper and an explanatory video are available at: https://citp.princeton.edu/research/voting/.

[8] For a partial bibliography of voting machine attack research, see: J. A Halderman, "Practical Attacks on Real-world E-voting." In F. Hao and P. Y. A. Ryan (eds.), *Real-World Electronic Voting: Design, Analysis and Deployment*, CRC Press, December 2016. Available at: https://jhalderm.com/pub/papers/ch7-evoting-attacks-2016.pdf.

[9] I explained how attackers can bypass these obstacles in a recent congressional briefing: *Strengthening Election Cybersecurity*, May 15, 2017. The video is available at https://www.electiondefense.org/congressional-briefings-cyber-security/.

[10] For a more detailed description of how adversaries might select targets, see J. A. Halderman, "Want to Know if the Election was Hacked? Look at the Ballots," November 2016, available at: medium.com/@jhalderm/want-to-know-if-the-election-was-hacked-look-at-the-ballots-c61a6113b0ba.

Our election infrastructure is not as distant from the Internet as it may seem.[11] Before every election, voting machines need to be programmed with the design of the ballot, the races, and candidates. This programming is created on a desktop computer called an election management system, or EMS, and then transferred to voting machines using USB sticks or memory cards. These systems are generally run by county IT personnel or by private contractors.[12] Unfortunately, election management systems are not adequately protected, and they are not always properly isolated from the Internet. Attackers who compromise an election management system can spread vote-stealing malware to large numbers of machines.[13]

Russian Attack Attempts: The Threats Are Real

The key lesson from 2016 is that hacking threats are real.

This month, we've seen reports detailing Russian efforts to target voter registration systems in up to 39 states[14] and to develop a capability to spread an attack from an election technology vendor to local election offices.[15] Attacking the IT systems of

---

[11] Fortunately, the U.S. has resisted widespread use of Internet voting—a development that would paint a fresh bull's eye on our democratic system. I myself have demonstrated attacks against Internet voting systems in Washington, D.C., Estonia, and Australia. See:
S. Wolchok, E. Wustrow, D. Isabel, and J. A. Halderman, "Attacking the Washington, D.C. Internet Voting System." In *Proceedings of the 16th Intl. Conference on Financial Cryptography and Data Security*, February 2012. Available at: https://jhalderm.com/pub/papers/dcvoting-fc12.pdf.
D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. Halderman, "Security Analysis of the Estonian Internet Voting System." In *Proceedings of the 21st ACM Conference on Computer and Communications Security* (CCS), November 2014. Available at: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf.
J. A. Halderman and V. Teague, "The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election." In *Proceedings of the 5th International Conference on E-voting and Identity*, September 2015. Available at: https://arxiv.org/pdf/1504.05646v2.pdf.
For a broader discussion of why secure Internet voting systems are likely decades away, see:
R. Cunningham, M. Bernhard, and J. A. Halderman, "The Security Challenges of Online Voting Have Not Gone Away." IEEE Spectrum, November 3, 2016. http://spectrum.ieee.org/tech-talk/telecom/security/the-security-challenges-of-online-voting-have-not-gone-away.

[12] In my own state, Michigan, about 75% of counties outsource pre-election programming to a pair of independent service providers. These are small companies with 10–20 employees that are primarily in the business of selling election supplies, including ballot boxes and "I Voted" stickers.

[13] See, for example, J. Calandrino, et al., "Source Code Review of the Diebold Voting System," part of the California Secretary of State's "Top-to-Bottom" Voting Systems Review, July 2007. Available at: https://jhalderm.com/pub/papers/diebold-ttbr07.pdf.

[14] M. Riley and J. Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known." *Bloomberg*, June 13, 2017. https://www.bloomberg.com/politics/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.

[15] M. Cole, R. Esposito, S. Biddle, and R. Grim, "Top-secret NSA Report Details Russian Hacking Efforts Days Before 2016 Election." *The Intercept*, June 5, 2017. https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.

vendors and municipalities could put the Russians in a position to sabotage equipment on election day, causing voting machines or electronic poll books to fail, resulting in long lines or other disruptions. The Russians could even have engineered this chaos to have a partisan effect, by targeting localities that lean heavily towards one candidate or another.

Successful infiltration of election IT systems also could have put the Russians in a position to spread an attack to the voting machines and potentially steal votes. Although the registration systems involved were generally maintained at the state level, and most pre-election programming is performed by counties or outside vendors, counties tend to be even less well defended than state governments. They typically have few IT support staff and little, if any, cybersecurity expertise.

Another approach that the Russians might have been planning is to tamper with the voting system in an obvious, easily discovered way, such as causing reporting systems to send the news media incorrect initial results on election night. Even if the problem was corrected and no actual votes were changed, this would cause uncertainty in the results and widespread distrust of the system, which would injure our democratic processes. If voters cannot trust that their votes are counted honestly, they will have reason to doubt the validity of elections.[16]

I don't know how far the Russians got in their effort to penetrate our election infrastructure, nor whether they interfered with equipment on election day. (As far as the public knows, no voting equipment has been forensically examined to check whether it was successfully attacked.) But there is no doubt that Russia has the technical ability to commit widescale attacks against our voting system, as do other hostile nations. As James Comey testified here two weeks ago, we know "They're coming after America," and "They'll be back."[17]

Practical Steps to Defend Election Infrastructure

We must start preparing now to better defend our election infrastructure and protect it from cyberattacks before the elections in 2018 and 2020. The good news is, we know how to accomplish this. Paper ballots, audits, and other straightforward steps can make elections much harder to attack.

---

[16] See, as one example, E. H. Spafford, "Voter Assurance." NAE *The Bridge*, December 2008. https://www.nae.edu/19582/Bridge/VotingTechnologies/VoterAssurance.aspx.

[17] Testimony of former FBI Director James B. Comey before the Senate Select Committee on Intelligence, June 8, 2017.

I have entered into the record a letter from over 100 computer scientists, security experts, and election officials. This letter recommends three essential measures that can safeguard U.S. elections:

- First, we need to replace obsolete and vulnerable voting machines, such as paperless systems, with optical scanners and paper ballots—a technology that 36 states already use. Paper provides a resilient physical record of the vote[18] that simply can't be compromised by a cyberattack. President Trump made this point well shortly before the election in an interview with Fox News. "There's something really nice about the old paper-ballot system," he said. "You don't worry about hacking. You don't worry about all the problems that you're seeing."[19]

- Second, we need to consistently and routinely check that our election results are accurate, by inspecting enough of the paper ballots to tell whether the computer results are right.[20] This can be done with what's known as risk-limiting audits.[21] Such audits are a common-sense quality control.[22] By manually checking a relatively small random sample of the ballots, officials can quickly and affordably provide high assurance that the election outcome was correct.

Optical scan ballots paired with risk-limiting audits provide a practical way to detect and correct vote-changing cyberattacks. They may seem low-tech, but they are a reliable, cost-effective defense.[23]

---

[18] Of course, paper ballots can be tampered with too, by people handling them. Optical scan tabulation has the advantage that it produces both paper and electronic records. As long as officials check that both sets of records agree, it would be very difficult for criminals to alter the election outcome without being detected, whether by a cyberattack or by old-fashioned ballot manipulation.

[19] See: http://www.businessinsider.com/donald-trump- election-day-fox-news-2016-11.

[20] At least 29 states already require some form of post-election audit. However, since the procedures in most states are not designed as a cyber defense, the number of ballots that are audited may be much too low or geographically localized to reliably detect an attack. Some states also allow auditing by rescanning paper ballots through the same potentially compromised machines. Results from paperless DRE voting machines cannot be strongly audited, since there is no physical record to check. For state-by-state details, see National Conference of State Legislatures, "Post-election Audits," June 2017. Available at: http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx.

[21] For a detailed explanation of risk-limiting audits, see J. Bretschneider et al., "Risk-Limiting Post-Election Audits: Why and How." Available at: https://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf. New Mexico already requires something similar to a risk-limiting audit, and Colorado is implementing risk-limiting audits starting in 2017. Risk-limiting audits have been tested in real elections in California, Colorado, and Ohio.

[22] One of the reasons why post-election audits are essential is that pre-election "logic and accuracy" testing can be defeated by malicious software running on voting machines. Vote-stealing code can be designed to detect when it's being tested and refuse to cheat while under test. Volkswagen's emission-control software did something similar to hide the fact that it was cheating during EPA tests.

[23] Former CIA director James Woolsey and Lt. Col. Tony Shaffer call for paper ballots and auditing in a May 12, 2017 op-ed in Fox News: "Ultimately, we believe the solution to election insecurity lies in

- Lastly, we need to raise the bar for attacks of all sorts—including both vote tampering and sabotage—by conducting comprehensive threat assessments and by applying cybersecurity best practices to the design of voting equipment[24] and the management of elections.

These fixes aren't expensive. Replacing insecure paperless systems nationwide would cost between $130 million and $400 million.[25] Running risk-limiting audits nationally for federal elections would cost less than $20 million a year.[26] These amounts are vanishingly small compared to the national security improvement the investment buys. Yet such measures could address a prime cyber challenge, boost voter confidence, and significantly strengthen a crucial element of our national security. They would also send a firm response to any adversaries contemplating interfering with our election system.

Election officials have an extremely difficult job, even without having to worry about cyberattacks by hostile governments. The federal government can make prudent and cost-effective investments to help them defend our election infrastructure and uphold voters' confidence. With leadership from across the aisle, and action in partnership with the states, our elections can be well protected in time for 2018 and 2020.

Thank you for the opportunity to testify. I look forward to answering any questions.

President Reagan's famous old adage: 'trust but verify'." http://www.foxnews.com/opinion/2017/05/12/america-s-voting-systems-need-security-upgrades-it-s-time-to-beef-up-cybersecurity.html.

[24] One notable effort to develop secure voting equipment is STAR-Vote, a collaboration between security researchers and the Travis County, Texas elections office. STAR-Vote integrates a range of modern defenses, including end-to-end cryptography and risk limiting audits. See S. Bell et al., "STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System." USENIX Journal of Election Technology and Systems (JETS) 1(1), August 2013. https://www.usenix.org/system/files/conference/evtwote13/jets-0101-bell.pdf.

[25] Brennan Center, "Estimate for the Cost of Replacing Paperless, Computerized Voting Machines," June 2017. https://www.brennancenter.org/sites/default/files/analysis/New_Machines_Cost_Across_Paperless_Jurisdictions%20%282%29.pdf. This cost might be significantly reduced by developing voting equipment based on open-source software and commercial off-the-shelf (COTS) hardware.

[26] This estimate assumes that auditing a federal race will have an average cost similar to manually recounting 10% of precincts. In a risk-limiting audit, the actual number of ballots that must be checked varies with, among other factors, the margin of victory.

Chairman BURR. Dr. Halderman, thank you.

The Chair would recognize himself for five minutes. Members will be recognized by seniority.

Secretary Lawson, in how many states is the secretary of state in charge of the elections process, do you know?

Ms. LAWSON. Yes, sir. It's 40.

I'm sorry. Yes, sir. It's 40.

Chairman BURR. Okay. Would you be specific: What do the secretary of states do—what is it they do not like about elections being designated critical infrastructure?

Ms. LAWSON. The most important issue, sir, is that there have been no clear parameters set and, even after the three calls that we had with Secretary Jeh Johnson before the designation was made, we consistently asked for what would be different if the designation was made and how we would communicate. Would it be any different——

Chairman BURR. So nothing has negatively happened except that you don't have the guidance to know what to do?

Ms. LAWSON. Nothing has negatively happened to this date, but also nothing positive has happened.

Chairman BURR. Got it. Got it.

Mr. Sandvoss, Illinois is one of the few states that have publicly been identified. I guess that's in part because you took the initiative to do it. You gave a good chronology: 23 June, first sign; 12 July, State IT staff took action; 12 August, the attacks stopped.

At what point was the State of Illinois contacted by any Federal entity about their system having been attacked or was it the State of Illinois that contacted the Federal Government?

Mr. SANDVOSS. We were contacted by the FBI—I don't have the exact date, but it was after we had referred the matter to the Attorney General's office. My guess would be probably a week after.

Chairman BURR. A week after——

Mr. SANDVOSS. After the AG was notified by us of this breach.

Chairman BURR. And the AG was notified approximately when?

Mr. SANDVOSS. On July 19th.

Chairman BURR. July 19th. Okay.

At what point did the State of Illinois know that it was the Russians?

Mr. SANDVOSS. Actually, to this day we don't know with certainty that it was the Russians. We've never been told by any official entity. The only one that we're aware of that was investigating was the FBI and they have not told us definitively that it was the Russians. Our IT staff was able to identify, I think it was, seven IP addresses from a foreign location, I believe it was The Netherlands. But that doesn't mean that the attack originated in the Netherlands. We have no idea where it originated from.

Chairman BURR. Did your IT staff have some initial assessments on their own?

Mr. SANDVOSS. No, because I think any—anything of that nature would have been speculative and we didn't want to do that. I think we wanted to leave that to the professional investigators.

Chairman BURR. You gave an update on what you're currently doing to enhance the security: DHS weekly security checks. Has

the Federal—in your estimation, has the Federal Government responded appropriately to date?

Mr. SANDVOSS. I believe they have, yes. I've heard nothing from our IT division and they'd be the persons that would know. I've heard nothing from them that the DHS's work in that matter has been less than satisfactory.

Chairman BURR. Let me ask all of you, except for you, Mr. Sandvoss: Do you believe the extent of cyber threats to election systems should be made public before the next election cycle? Should we identify those states that were targeted, Mr. Haas?

Mr. HAAS. I think as election directors we're certainly sensitive to the balance that Homeland Security and others need to make. I think so far, as far as we've gone, we want to know as the victims or potential victims. And then I think as part of the coordinating council and designation of critical infrastructure, there has to be a conversation amongst the election——

Chairman BURR. Is there a right of the public in your State to know?

Mr. HAAS. Yes, I believe there is. If there was a hack into our system, I think that we would certainly want to consult our statutes and so forth, but we would—we believe in transparency. We would want to let the public know.

Chairman BURR. Dr. Halderman.

Dr. HALDERMAN. I think the public needs details about these attacks and about the vulnerabilities of the system, in order to make informed decisions about how we can make the system better and to provide the resources that election officials need. So, yes.

Chairman BURR. Okay.

Secretary Lawson.

Ms. LAWSON. I lay awake at night worrying about public confidence in our election systems, and so I think we need to be very careful and we need to balance the information, because the worst thing that we can do is make people think that their vote doesn't count or it could be canceled out.

And so if telling the public that, you know, that these attacks are out there and our systems are vulnerable and it doesn't undermine confidence, it makes them know that we are doing everything we possibly can to stop those attacks, I'd be in favor of it.

Chairman BURR. I take for granted none of you at the table have evidence that vote tallies were altered in the 2016 election?

Dr. HALDERMAN. Correct.

Chairman BURR. Dr. Halderman, before I recognize the Vice Chairman real quickly: When you and your colleagues hacked election systems, did you get caught?

Dr. HALDERMAN. We hacked election systems as part of academic research, where we had machines in our facilities——

Chairman BURR. I get that. Did you get caught? Did they see your intrusion into their systems?

Dr. HALDERMAN. The one instance when I was invited to hack a real voting system while people were watching, was in Washington, D.C., in 2010, and in that instance it took less than 48 hours for us to change all the votes and we were not caught.

Chairman BURR. Vice Chairman.

Vice Chairman WARNER. I'd like to thank all the witnesses for their testimony. I find a little stunning, Mr. Sandvoss, your answer. I don't know—I think if you saw the preceding panel, you had the DHS and the FBI unambiguously say that it was the Russians who hacked into these 21 systems, and I find it a little strange that they've not relayed that information to you.

What we discovered in the earlier testimony is that we finally got public disclosure that 21 states were attacked, and under questioning from Senator Harris we found that, even though we know those 21 states were attempted to be hacked into, or doors rattled or whatever analogy you want to use, in many cases the State election officials, whether the State directors or the secretaries of state, may not even have been notified.

I find that stunning. And clearly lots of local elected officials, local election officials, where the activities really take place, haven't been notified. So I've got a series of questions and I'd ask for fairly brief responses.

Dr. Halderman, can you just again restate—as Senator King mentioned in the earlier testimony, you don't need to disrupt a whole system. You could disrupt a single jurisdiction in a State, and if you could in effect wipe that ledger clean, you could invalidate potentially not just that local election, but then the results at the State, the Congressional level, the states, and ultimately the Nation, is that not correct?

Dr. HALDERMAN. Yes, that's correct.

Vice Chairman WARNER. So we are not—while it's important and I believe in our decentralized system, we are only as strong as our weakest link. Is that not correct?

Dr. HALDERMAN. That's correct.

Vice Chairman WARNER. Mr. Haas and Secretary Lawson, do you believe that all 21 states that were attacked, that the State election officials are aware?

Ms. LAWSON. I can't answer that question, sir. I'm not certain. I will tell you that Indiana has not been notified. I don't know if we're even on the list.

Mr. HAAS. I don't know for sure, except that DHS did indicate in a teleconference that all the states that were attacked have been notified.

Vice Chairman WARNER. We were told earlier that that's not the case. We were told that they may have been—the vendors may have been notified. So do you know whether Wisconsin was attacked?

Mr. HAAS. We have not been told that we were—that there was an attack on Wisconsin.

Vice Chairman WARNER. Are you comfortable, either one of you, with not having that knowledge?

Ms. LAWSON. We are hypersensitive about our security and I would say that when the FBI sent the notice in September for states to look for certain IP addresses to see if their systems had been penetrated or attempted to be penetrated, we absolutely searched. In fact, we looked at 15,500,000 log-ins that had happened in our system since the 1st of January that year. So we believe that our system has not been hacked.

Mr. HAAS. I would also state that both our office and the chief information officer of the State and his office would likely be able to detect if the system was hacked.

Vice Chairman WARNER. Well just, we've got the two leading State election officials not knowing whether their states were one of the 21 that at least the Russians probed—let me finish, please. And you know, I see—I understand the balance. But the notion that State election officials wouldn't know, that local election officials clearly haven't been notified—I appreciate the Chairman's offer. The Chairman and I are going to write a letter to all the states: If you view yourself as victims, I think there is a public obligation to disclose. Again, not to re-litigate 2016, but to make sure that we're prepared for 2017, where I have State elections in my State this year, and 2018. And to do otherwise—because there are some, there are some still in the political process, that believe this whole Russian incursion into our elections is a witch hunt and fake news.

So I could very easily see some local elected officials saying: "This is not a problem, this is not a bother; I don't need to tighten up my security procedures at all." And that would do a huge, huge disservice to the very trust, Secretary Lawson, that you say you want to try to present and provide for our voters.

So I hope when you receive the letter from our—and we'll write this on a confidential basis, but that you would urge your colleagues to come forward, again not to embarrass any State. But I find it totally unacceptable, one, that the public doesn't know, that local elected officials—local election officials don't know, that you as two, as the leaders of the State election officials, don't even know whether your states were part of the 21 that has been testified by the DHS that at least they were, if not looked at, door jiggled, or actually, as the case in Illinois, where actual information from the voter registration efforts were exfiltrated.

So my hope is that you will work with us on a cooperative basis and we want to make sure that the DHS and others are better at sharing information and you get those classified briefings that you deserve.

Chairman BURR. Senator Risch.

Senator RISCH. Thank you very much.

Mr. Sandvoss, July 12th was the date that you first discovered that you had issues, is that right?

Mr. SANDVOSS. Yes, that's correct.

Senator RISCH. And that was a result of a high-volume spike. Is that correct?

Mr. SANDVOSS. Yes, that is correct.

Senator RISCH. Then when you looked at it, you found out that the intrusion attempts actually had started June 23rd, is that correct?

Mr. SANDVOSS. Yes.

Senator RISCH. So—and those were low-volume spikes, starting on June 23rd?

Mr. SANDVOSS. Yes.

Senator RISCH. All right. So if they had never cranked up the volume, is it fair to say you would have never discovered it or probably wouldn't have discovered it?

Mr. SANDVOSS. I would say it would probably not have been discovered, certainly not right away. And if it was—the volume was low enough, even an analysis of our server logs might not catch something like that, because it wouldn't stand out. So I think the answer to your question is yes.

Senator RISCH. Then you said 12—or seven days later, the 19th, you notified the Attorney General. Is that right?

Mr. SANDVOSS. Yes, correct.

Senator RISCH. That was the Illinois Attorney General, not the U.S. Attorney General, is that correct?

Mr. SANDVOSS. Yes. State law requires that we notify the Attorney General in these instances.

Senator RISCH. So then the next thing that happened is you were contacted by the FBI. Is that correct?

Mr. SANDVOSS. Yes.

Senator RISCH. All right. So the question I've got—I'm just trying to get an understanding of the facts—are you assuming that the Illinois AG contacted the FBI, or do you know that or not know that, or——

Mr. SANDVOSS. I don't know that for sure, but I would suspect that they probably did, because how else would the FBI know?

Senator RISCH. Right. Well, and that's kind of where I was getting, is that was not the result of some Federal analysis, that there wasn't a Federal analysis of this that turned up what had actually happened. Is that a fair statement?

Mr. SANDVOSS. I believe so, yes.

Senator RISCH. Okay. You then did some things to try to mitigate what had happened. Have you shared this with other states as to what you had done, in order to, I don't know, develop a best practices, if you would?

Mr. SANDVOSS. We didn't have any formal notification to all 50 states, no. I think our focus at that time was trying to repair the damage and assess, you know, what needed to be done, especially with respect to the voters who had their information accessed.

I believe that once the FBI became aware of this, I know they contacted the different states. I don't believe our Attorney General's office did, although I don't know that for certain. But we did not have any formal communication with all 50 states regarding this.

Senator RISCH. And do you believe that you have developed a best-practices action after this attack that you've described for us?

Mr. SANDVOSS. I believe so, yes.

Senator RISCH. Do you think it would be appropriate for you to get that out through the secretary of states organization or other organizations, so that other states could have that?

Mr. SANDVOSS. Certainly. Absolutely.

Senator RISCH. Okay.

Mr. Halderman, Your hacking that you've described for us, would your ability—if you were sitting in Russia right now and wanted to do the same thing that you had done, would that ability be dependent upon the machines or whatever system is used being connected to the Internet?

Dr. HALDERMAN. That ability would depend on whether pieces of election IT equipment, IT offices that are where the election pro-

gramming is prepared, are ever connected to Internet. The machines themselves don't have to be directly connected to the Internet for a remote attacker to target them.

Senator RISCH. So would you recommend that the voting system be disconnected from the Internet, that it be a standalone system that can't be accessed from the outside?

Dr. HALDERMAN. It's a best practice, certainly, to isolate vote tabulation equipment as much as possible from the Internet, including isolating the systems that are used to program it.

But other pieces of election infrastructure that are critical, such as electronic poll books or online registration systems, do sometimes need to be connected to Internet—to systems that have Internet access.

Senator RISCH. But that wouldn't necessarily require that it be connected to the Internet for the actual voting process. Is that right?

Dr. HALDERMAN. That's right.

Senator RISCH. And then the extrication of that information off of the voting machine, would that be fair?

Dr. HALDERMAN. I think that's fair to say.

Senator RISCH. Thank you.

Mr. Chairman, I think all of this really needs to be drilled down a little bit further, because it seems to me, with this experience, there's probably some pretty good information where you could put a firewall in place to stop it, or at least minimize it.

Thank you.

Chairman BURR. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman. And thank all of you.

I want to start with you, Professor Halderman. What are the dangers of manipulation of voter registration databases, particularly if it isn't apparent until Election Day when people show up at the polls to vote?

Dr. HALDERMAN. I'm concerned that manipulating voter registration databases could be used to try to sabotage the election process on Election Day. If voters are removed from the registration database and then they show up on Election Day, that's going to cause problems. If voters are added to the voter registration database, that could be used to conduct further attacks.

Senator WYDEN. Let me ask—and this can be directed at any of you. I'm trying to get my arms around this role of contractors and subcontractors and vendors who are involved in elections. Any idea, even a ball park number, of how many of these people there are? 10, 70, 200?

Dr. HALDERMAN. Vendors that host the voter registration system?

Vice Chairman WARNER. Yes.

Dr. HALDERMAN. I'm sorry, Senator, I don't have a number.

Ms. LAWSON. Sir, I don't have an exact number either, but I will tell you, in Indiana, for an example, we have six different voting system types. Counties make that decision on their own. But they are all certified by our voting system technical oversight program.

Senator WYDEN. That was my main question. So somebody is doing certification over these contractors and subcontractors and

equipment vendors and the like? Does that include voting machines, by the way?

Ms. LAWSON. It does. Most states will have a mechanism to certify the voting machines that they're using, the electronic poll books they're using, the tabulation machines that they're using, making sure that they comply with Federal and State law, and making sure that they have the audit processes in place.

Senator WYDEN. So do you all have a high degree of confidence that these certification processes are not leaving this other world of subcontractors and the like vulnerable?

Dr. HALDERMAN. I have several concerns about the certification processes, including that some states do not require certification to Federal standards; that the Federal standards that we have are unfortunately long overdue for an update and have significant gaps when it comes to security; and that the certification process doesn't necessarily cover all of the actors that are involved in that process, including the day-to-day operations of companies that do pre-election programming.

Senator WYDEN. One last question. We Oregonians and a number of my colleagues are supportive of our efforts to take vote-by-mail national. And we've had it. I was in effect the country's first Senator elected by vote-by-mail in 1996. We've got a paper trail. We've got air gap computers. We've got plenty of time to correct voter registration problems if there are any.

Aren't those the key elements of trying to get on top of this? Because it seems to me, particularly the paper trail—if you want to send a message to the people who are putting at risk the integrity of our electoral institutions, having a paper trail is just fundamental to being able to have the backup we need.

I think you're nodding affirmatively, Professor Halderman, so I'm kind of inclined—or one of you two at the end were nodding affirmatively, and I'll quit while I'm ahead if that was the case. But would either of you like to take that on?

Dr. HALDERMAN. Vote-by-mail has significant cybersecurity benefits. It's very difficult to hack a vote-by-mail system from an office in Moscow. Whether vote-by-mail is appropriate for every State in every context is in our system of course a matter for the states, but I think it offers positive security benefits.

Senator WYDEN. All right.

Thank you, Mr. Chairman.

Chairman BURR. Senator Blunt.

Senator BLUNT. Dr. Halderman, on that last answer to that last question, how do you count vote-by-mail ballots?

Dr. HALDERMAN. Generally, they would be counted using optical scanners.

Senator BLUNT. Exactly. So you count them the same way you count ballots that aren't vote-by-mail in almost every jurisdiction?

Dr. HALDERMAN. If the optical scan ballots are subsequently audited, you can get high security from that process, but yes.

Senator BLUNT. Well that's a different—that's a different question. Your question there is do you prefer paper ballots and an audit trail, and I do too. But let's not assume that the vote-by-mail ballots are counted any differently. They're counted probably at a more central location, but that doesn't mean that all the manipula-

tion you talked about that we need to protect against wouldn't happen in a vote-by-mail election. You've got a way to go back and you've got a paper trail to count.

Dr. HALDERMAN. That's correct. There are three things you need: paper, auditing, and otherwise good security practices.

Senator BLUNT. While I've got you there, on auditing, how would you audit a non-paper system? If it's a touchscreen system—you mentioned Colorado, and New Mexico already did a required sample audit, which I'm certainly not opposed to that if that's what states want to do, or it's the best thing to do. How would you do a non-paper audit?

Dr. HALDERMAN. Senator, I think it would be difficult or impossible to audit non-paper systems with the technology that we use in the United States to a high level of assurance.

Senator BLUNT. So even if you—if you don't have something to audit, it's pretty hard to audit a system that counted—that didn't leave a trail.

Dr. HALDERMAN. It's basically impossible.

Senator BLUNT. So, Mr. Sandvoss, in Illinois do you certify counting systems?

Mr. SANDVOSS. Yes, we do.

Senator BLUNT. And Secretary Lawson, do you certify counting systems?

Ms. LAWSON. Yes, sir.

Senator BLUNT. Mr. Haas, in your, your jurisdiction, somebody is certifying those systems that you use?

Mr. HAAS. We both rely on the EAC certification and then our commission does a testing protocol and then approves the equipment to be used in the State of Wisconsin.

Senator BLUNT. And back in Illinois, do you then monitor in any way that counting system while it's doing the actual counting?

Mr. SANDVOSS. No, the actual counting done on Election Day, Election Night rather, is done locally at the county clerk's offices or board of election commissioner offices. We certify the voting equipment. They have to apply for certification and approval, which we conduct a fairly rigorous test of the voting equipment. But then in actual practice, other than—we do conduct pre-election tests of the voting equipment on a random basis before each election, but there—it's a limited number of jurisdictions.

Senator BLUNT. And do you do that in a way that allows you from your central office to get into the local system? Or do you go to the local jurisdictions or just monitor how they count that—how they, how they check that counting system?

Mr. SANDVOSS. When we do our pre-election tests, we actually visit the jurisdiction.

Senator BLUNT. All right.

Secretary Lawson, similar?

Ms. LAWSON. Similar. However, the State does not go into the counties, but the counties are required to do a public test and, as I mentioned, it's public. And so they're required to do testing on the machines, the tabulation. There's a bipartisan election board that's there——

Senator BLUNT. I guess the point I'd want to drive home there is that not opening that door to the counting system—if you don't

have the door, nobody else can get through that door as well. But there's monitoring, there's local testing.

I don't suggest at all that Dr. Halderman's comments aren't important or something we should guard against. I was an election official for 20 years, including the chief election official for 8 of those, and something—as we were transitioning to these systems, something I was always concerned about is what could possibly be done that could be done and undetected.

One of the reasons I always liked the audit trail—that obviously, Dr. Halderman, you do, you do too, is that you do have something to go back, if you have a reason to go back, and really determine what happened on Election Day.

Let's talk for just a moment about the much more open registration system. Secretary Lawson, you said you had 15,500 logins. I believe that was—talk about logging—what are they logging into there? The statewide voter registration system that you maintain a copy of?

Ms. LAWSON. The 92 county clerks in Indiana are connected to the statewide voter registration system, and that 15,500,000 logins reflected the work that they did that year.

Senator BLUNT. 15,500,000?

Ms. LAWSON. 15,500,000.

Senator BLUNT. So obviously that's a system that has lots of people coming in and out of that system all the time. Do local jurisdictions, like if the library does registration, do you have counties where they can also put those registrations directly into the system?

Ms. LAWSON. Other than the counties, no, sir. But we do have Indianavoters.com, where a voter can go on and register themselves. And it's a record that is compared to the DMV record, and then the counties will find that information in their hopper the next day. And then they will—or their computer system, and then the next day they will have the ability to determine whether or not the application is correct.

Senator BLUNT. Do all of your jurisdictions, the three jurisdictions here reflected, have some kind of provisional voting? If you get to the voting place on Election Day and your address is wrong, or your name is wrong, or it doesn't occur—it doesn't appear at all, do you have a way somebody can cast a ballot before they leave?

Ms. LAWSON. Yes, sir.

Senator BLUNT. And in Illinois?

Mr. SANDVOSS. Yes, we do.

Mr. HAAS. We have provisional ballots, but they are very limited. We are not an NVRA State. And we also have Election Day registration, so people can register at the polls.

Senator BLUNT. So, the failure to have your name properly on the—I understand, Chairman, and I also noticed the time on others. But just, the registration system is much more open than the tallying system, that doesn't mean the tallying system doesn't need to be further protected. But the registration system, the idea that somebody gets into the registration system—there are plenty of ways to do that. Unfortunately, we think now other countries and governments may be doing that as well.

Chairman BURR. Senator King.

Senator KING. Thank you, Mr. Chairman.

Dr. Halderman, you're pretty good at hacking voting machines, by your testimony. Do you think the Russians are as good as you?

Dr. HALDERMAN. The Russians have the resources of a nation state. I would say their capabilities would significantly exceed mine.

Senator KING. I expected that was going to be your answer, but I wasn't sure whether your modesty would—but I think that's an important point, because you testified here today that you were able to hack into a voting machine in 48 hours, change the results, and nobody knew you had done it. And if you could do it, I think the point is the Russians could do it if they chose.

And we've been talking a lot about registrations lists. My understanding is that quite often a voter registration list at some point in the process is linked up with—the computer that has the voter registration list is linked up with configuring the voting machines, and perhaps even tallying votes. Is that true? Can any of you——

Ms. LAWSON. No, sir.

Senator KING. There's no connection between the registration list and the voting machines?

Ms. LAWSON. No.

Senator KING. Illinois? Is that——

Mr. SANDVOSS. Not in Illinois, no.

Senator KING. Okay.

Mr. HAAS. That's correct.

Senator KING. Then I was mistaken.

Yes, Dr. Halderman?

Dr. HALDERMAN. I believe that depends on the specific equipment involved. There may be some designs of voting systems where the sign-in and the vote counting system are linked.

Senator KING. But of course, if, as you testified I think, if the voting registration list is tampered with in some way on Election Day, it would be chaos if names disappeared, people arrived at the polls and their names weren't on the list. Isn't that correct, Ms. Lawson?

Ms. LAWSON. If a person showed up at the polls to vote and their name wasn't on the list, if they were expecting they would be given a provisional ballot, I think the biggest danger is that the lines at the polls would increase significantly if there was a large number of folks who had to do that in each precinct.

Senator KING. Right, that was what I was referring to.

On August 1 of 2016, press reports have indicated that there was an FBI notification to all of their field offices about the danger of cyber intrusions into voting systems. Supposedly, those were passed on to State election systems. Did you three get something from the FBI around August 1st that gave IP addresses and some warnings about what should be done?

Mr. SANDVOSS. Yes, we did receive an FBI flash. It was in August, and you're saying the 1st. I believe that was it.

Senator KING. That was, yes, I understand that was the date of it. Ms. Lawson, did you receive that?

Ms. LAWSON. Yes, Indiana received a notice from the FBI.

Mr. HAAS. We did as well.

Senator KING. So there is some interconnection. I mean, one of the things that I'm sort of hearing, and I'm frankly appreciative and happy that you all did receive that notice, but there seems to be a lack of information-sharing that goes on that we really need to be sure that—for example, if you learn—if something happens in Illinois, some system whereby you can alert your colleagues across the country to look out for this. And if we learn things here in Washington, if the FBI learns things, that they can alert people around the country, because the best time to deal with this is before the election. After the election or on Election Day is much more difficult.

Dr. Halderman.

Dr. HALDERMAN. Yes, I would support further information sharing.

Senator KING. And then finally, we've talked about what we do about this. Paper trails has come up. Is that the principal defense? Is that—Dr. Halderman, what if—I asked the question to the prior panel. What would you tell my elections clerk in Brunswick, Maine, would be the three things most important that they should do, or my Secretary of State in Maine, to protect themselves against a threat we know is coming?

Dr. HALDERMAN. The most important things are to make sure we have votes recorded on paper, paper ballots, which just cannot be changed in a cyber attack, that we look at enough of that paper in a post-election, risk-limiting audit, to know that they haven't—the electronic records haven't been changed; and then, to make sure we are generally increasing the level of our cyber security practice. Information-sharing is an example of a good and recommended practice, as are firewalling systems and other things that have been suggested.

Senator KING. One final question. Is it possible—and there are some press reports about this—a cyber attack on the vendors of these machines, to somehow tamper with the machines before they go out to the states. Is that a risk?

Dr. HALDERMAN. I would be concerned about that. And in fact the small number of vendors is an example of how our system in practice is not quite as decentralized as it may appear, that attacks spreading via vendors or from vendors to their customers could be a way to reach voting equipment over a very large area.

Senator KING. And there have been press reports that that in fact, was attempted in 2016.

Dr. HALDERMAN. Yes, that's correct.

Senator KING. Thank you, Mr. Chairman. Mr. Chairman, I want to thank you for holding this hearing. This is such important information for the public and for our democracy. I appreciate your work here.

Chairman BURR. Thank you, Senator.

Senator Harris.

Senator HARRIS. Thank you.

So there's a saying that I'm sure many of you have heard, which is the you know the difference between being hacked and not being hacked, is knowing you've been hacked. And so I appreciate, Dr. Halderman, the recommendations that you and your colleagues have made, because it also seems to cover the various elements of

what we need to do to protect ourselves as a country in terms of our elections, which is prevention, and then there's the issue of detection and also resilience. Once we—if we discover that we've been manipulated, let's have the ability to stand back up as quickly as possible.

So I have a few questions in that regard. First of all, have each of you—you received for the states, received a notification from the FBI? Is that correct?

Ms. LAWSON. Yes, ma'am.

Mr. HAAS. Yes, yes.

Mr. SANDVOSS. Yes.

Senator HARRIS. And were any of you also notified by DHS? Mr. Sandvoss?

Mr. SANDVOSS. We've had communications with DHS. I don't recall how they were initiated. But I do know that there have been some conference calls with them, and it may have been through the FBI that that occurred.

Senator HARRIS. And I'm speaking of before the 2016 election.

Mr. SANDVOSS. Yes.

Senator HARRIS. Yes.

Mr. SANDVOSS. Yes.

Senator HARRIS. Secretary Lawson.

Ms. LAWSON. Yes, we had—we did have conversations with Department of Homeland Security. However, it was through our national association. It was not a direct contact with the State.

Senator HARRIS. Thank you.

Mr. HAAS. We were one of the states that took up DHS on their offers to do the cyber hygiene scan. We did have a number of communications with, I believe, a point person in their Chicago office. The FBI alert I think was about a specific incident, but our communications with DHS were more about general steps that could be taken to protect our systems.

Senator HARRIS. So as a follow-up to this hearing, if each of you, to the extent that you can recall the nature of those conversations with DHS before the election, if you could share that with the Committee that would be helpful, so we can figure out how notifications might be more helpful to you in the future. Hopefully they're not necessary, but if necessary.

Can you, Ms. Lawson, tell me—Secretary Lawson—what in your opinion are the pros and cons of requiring states to report to the Federal Government if there's been a breach or a hack? What can you imagine would be the pros and cons of a policy that would require that?

Ms. LAWSON. Well, the pro would be that if there—if, for an example, the FBI or the Department of Homeland Security has better ways to counter those attacks, or to make sure that the reconnaissance that's done after such an attack is more sophisticated than the states, then obviously that would be a pro.

Indiana did not take the opportunity to have DHS do our cyber cleaning because we felt that we were in better shape than what they could provide for us, so that would be the con.

Senator HARRIS. Okay.

And can you, Professor Halderman, tell me—you know, before this last election cycle, there had been a lot of talk through the

years in various states—Senator Blunt, I'm sure you were part of those discussions—about the efficacy of online voting, because it would bring convenience, speed, efficiency, accuracy. And now we can see that there will be great, potentially, vulnerabilities by doing that. So can you talk with me a little about, just in terms of policy, is the day of discussing the need for online voting, has that day passed because of the vulnerabilities that are associated with that?

Dr. HALDERMAN. I think that online voting, unfortunately, would be painting a bullseye on our election system. Today's technology just does not provide the level of security assurance for an online election that you would need in order for voters to have high confidence.

And I say that having myself done—hacked an online voting system that was about to be used in real elections, having found vulnerabilities in online voting systems that are used in other countries. The technology just isn't ready for use.

Senator HARRIS. And isn't that the irony, that the professor of computer engineering and I, who always believed that we need to do more to adopt technology, that government needs to adopt technology, I think we're advocating the good old days of paper voting are the way to go, or at least an emphasis on that, instead of using technology to vote.

Can you tell me also—any of you, if you know—it's my understanding that some of the election system vendors have required states to sign agreements that prevent or inhibit independent security testing. Are you familiar with that?

Dr. HALDERMAN. That certainly had been something that inhibited attempts by researchers like me to study election systems in the past.

Senator HARRIS. And do you believe that that's a practice that is continuing?

Dr. HALDERMAN. I do not—I don't know the answer to that question.

Senator HARRIS. Have any of you had that experience with any of your vendors?

Mr. SANDVOSS. In Illinois, no, we have not. And I don't think Illinois law would allow such an agreement.

Ms. LAWSON. I don't believe that would happen in Indiana either, Senator, because in order to sell voting equipment in the State of Indiana it has to be certified.

Senator HARRIS. Right, which would require testing.

Ms. LAWSON. Yes, which requires testing.

Senator HARRIS. Thank you.

Thank you, Mr. Chairman. Thank you.

Chairman BURR. Thank you, Senator Harris.

Does any Senators seek additional questions or time?

[No response.]

Seeing none, let me wrap up. I want to thank all of you for your testimony today.

Secretary Lawson, to you. I really encourage you, as the next representative of secretaries of states, to remain engaged with the Federal Government, specifically the Department of Homeland Security. And I think with any transition of an administration there

is a handoff and a ramp-up. And I've been extremely impressed with our witness from DHS, who not only was here today, but she has taken the bull by the horns on this issue. And I think you'll see those guidelines very quickly, and I hope that there will be some interaction between secretaries of states, since in 40 states you control the voting process, and you can find a system of Federal guidance and collaboration that works comfortably with every secretary of state in your organization.

I think it is absolutely critical that we have not only a collaboration, but a communication, between the Federal Government and the states as it relates to our voting systems. If not, I fear that there would be an attempt to in some way, shape, or form nationalize that. That is not the answer.

And I'll continue to point, Mr. Sandvoss, to Illinois as a great example of a State that apparently focused on the IT infrastructure and staff, and didn't wait for the Federal Government to knock on the door and say, hey, you got a problem. You identified your problem, you began to remediate it. At some point, the Federal Government came in as a partner. And I think where we see our greatest strength is to work with states and to chase people like you, Dr. Halderman, who like to break into—no, I'm just kidding with you.

Listen, I think what you did is important. And I think the questions that you raised about the fact that you really can target to make the impact of what you're trying to do very, very effective. And that's clearly what campaigns do every day. So we shouldn't be surprised if the Russians actually looked at that or anybody else who wants to intrude into our voting system and our democracy in this country.

I've got to admit that the variation of voting methods, six in Indiana, where I don't know how many counties you've got—I've got 100 counties in North Carolina. It may be that I find out that every county in North Carolina has the power to determine what voting machines, what voting software they have.

This can get extremely complicated. Short of trying to standardize everything, which I don't think is the answer, is how do we create the mechanism for the Federal Government to collaborate directly with those heads of election systems in the states and understand up front what we bring to the table and how we bring it, so that we're all looking at the same thing—the integrity of every vote going to exactly who it was intended to do.

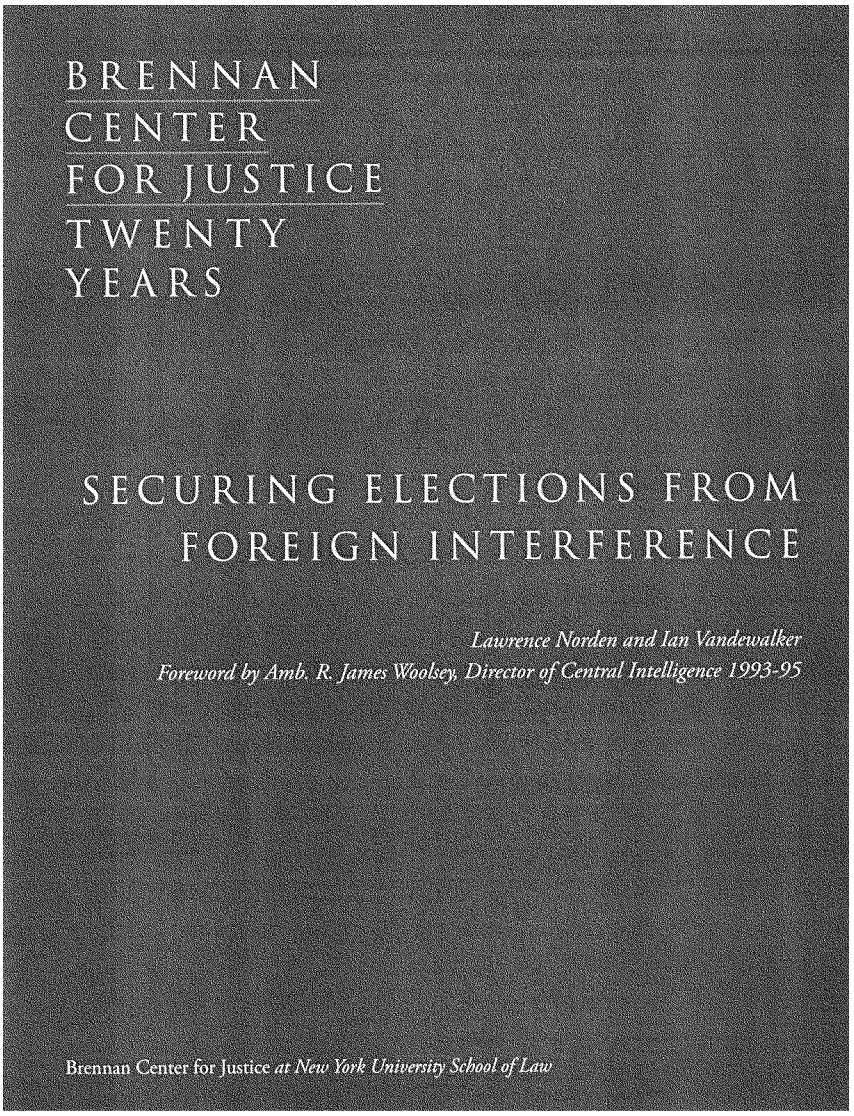
So, yes, we're going to have debates on paper or electronic. We're going to have debates on what should the Federal role be. At the end of the day, if we haven't got cooperation and collaboration and communication, I will assure you we will be here with another Congress, with another makeup of the Committee, asking the same questions, because we won't have fixed it.

But I think that what Dr. Halderman has said to us is, there are some ways that we can collectively approach this to where our certainty of intrusions in the future can go down and the accuracy of the vote totals can be certified.

So I thank all the four of you for being here today in our second panel. This hearing is now adjourned.

[Whereupon, at 12:36 p.m., the hearing was adjourned.]

Supplemental Material


BRENNAN
CENTER
FOR JUSTICE
TWENTY
YEARS
SECURING ELECTIONS FROM
FOREIGN INTERFERENCE
Lawrence Norden and Ian Vandewalker
Foreword by Amb. R. James Woolsey, Director of Central Intelligence 1993-95
Brennan Center for Justice at New York University School of Law

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. We work to hold our political institutions and laws accountable to the twin American ideals of democracy and equal justice for all. The Center's work ranges from voting rights to campaign finance reform, from ending mass incarceration to preserving Constitutional protection in the fight against terrorism. Part think tank, part advocacy group, part cutting-edge communications hub, we start with rigorous research. We craft innovative policies. And we fight for them — in Congress and the states, the courts, and in the court of public opinion.

ABOUT THE BRENNAN CENTER'S DEMOCRACY PROGRAM

The Brennan Center's Democracy Program works to repair the broken systems of American democracy. We encourage broad citizen participation by promoting voting and campaign finance reform. We work to secure fair courts and to advance a First Amendment jurisprudence that puts the rights of citizens — not special interests — at the center of our democracy. We collaborate with grassroots groups, advocacy organizations, and government officials to eliminate the obstacles to an effective democracy.

ABOUT THE BRENNAN CENTER'S PUBLICATIONS

Red cover | Research reports offer in-depth empirical findings.
Blue cover | Policy proposals offer innovative, concrete reform solutions.
White cover | White papers offer a compelling analysis of a pressing legal or policy issue.

ABOUT THE AUTHORS

Lawrence Norden is Deputy Director of the Brennan Center's Democracy Program. He has authored several nationally recognized reports and articles related to voting rights and voting technology, including *America's Voting Machines at Risk* (September 2015), *How to Fix Long Lines* (February 2013), *Better Design, Better Elections* (July 2012), and *Voting Law Changes in 2012* (October 2011). His work has been featured in media outlets across the country, including *The New York Times*, *The Wall Street Journal*, Fox News, CNN, MSNBC, and NPR. He has testified before Congress and several state legislatures on numerous occasions. He received his J.D. from New York University School of Law.

Ian Vandewalker serves as Senior Counsel for the Brennan Center's Democracy Program, where he works on voting rights and campaign finance reform. His work includes *Stronger Parties, Stronger Democracy: Rethinking Reform* (September 2015), a recurring series analyzing spending in U.S. Senate elections, and academic articles in the fields of election law and civil liberties. Press outlets across the nation have featured his work, including *The New York Times*, *The Washington Post*, and NPR. He earned his J.D. cum laude in 2008 from New York University School of Law and holds a master's degree in philosophy from Indiana University and a bachelor's degree from New College of Florida.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the many colleagues that collaborated in preparing this report. Brennan Center President Michael Waldman and Director of the Brennan Center's Democracy Program Wendy Weiser supplied an indispensable source of leadership and vision at all stages of this project. Brennan Center Vice Presidents Vivien Watts and John Kowal provided instrumental guidance and direction. Christopher Famighetti contributed crucial research and editorial support to this project. Raffe Jefferson and Rebecca Autrey of the Brennan Center's Communications Team lent valuable review and editing assistance. Brennan Center Senior Editor Jim Lyons provided helpful revisions. The authors are grateful to Ava Mehta for her important research. Research and Program Associate Phoenix Rice-Johnson and Democracy Program Intern Peter Dunphy merit special thanks for their sustained assistance in researching, fact-checking, and editing.

We are also immensely grateful to the many experts and officials whose knowledge and views helped shape this report. We sincerely thank the following individuals for generously sharing their expertise and information through multiple interviews: Matt Masterson, Commissioner, U.S. Election Assistance Commission; Merle King, Executive Director, Center for Election Systems at Kennesaw State University; David Becker, Director, Election Initiatives, Pew Charitable Trusts; Rebecca Wright, Professor of Computer Science at Rutgers University and Director of the Center for Discrete Mathematics and Theoretical Computer Science; Edgardo Cortes, Commissioner, Virginia Department of Elections; Matt Damschroder, Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio; Douglas Kellner, Co-Chair, State Board of Elections, New York; Jeremy Epstein, Deputy Division Director, Computer & Network Systems Division, National Science Foundation; Marian Schneider, Special Advisor to the Governor on Election Policy, Pennsylvania; Alex Halderman, Director, Center for Computer Security and Society, University of Michigan; Stuart Holmes, Voting Information System Manager, Secretary of State, Washington; Marc Burris, IT Director and CIO, State Board of Elections, North Carolina; Maggie Toulouse Oliver, Secretary of State of New Mexico; and Neil Jenkins, Chief of Policy and Planning, Department of Homeland Security, National Protection and Programs Directorate, Office of Cybersecurity & Communications.

This report also benefitted from the many willing to share their valuable experience and provide insight in the review process. Alongside many of the aforementioned experts, we gratefully acknowledge the following individuals for their helpful feedback: Pamela Smith, President, Verified Voting; Amb. R. James Woolsey; Justin Talbot-Zorn, Policy and Legislative Outreach Director, National Election Defense Coalition; and Ronald L. Rivest, Vannevar Bush Professor of Electrical Engineering and Computer Science, Massachusetts Institute of Technology.

The Brennan Center gratefully acknowledges Arkay Foundation, Bohemian Foundation, Carnegie Corporation of New York, Change Happens, Democracy Alliance Partners, Ford Foundation, Lisa and Douglas Goldman Fund, The Charles Evans Hughes Memorial Foundation, Audrey and Sydney Irmas Charitable Foundation, The JPB Foundation, Kohlberg Foundation, Inc., The Leon Levy Foundation, John D. and Catherine T. MacArthur Foundation, The Mertz Gilmore Foundation, Open Society Foundations, The Overbrook Foundation, PARC Foundation, Rockefeller Brothers Fund, The Schooner Foundation, Vital Projects Fund, Wallace Global Fund, and The WhyNot Initiative for their generous support of our money in politics and elections work.

TABLE OF CONTENTS

FOREWORD

By Amb. R. James Woolsey, Director of Central Intelligence 1993-95

In the last few months, we have learned extraordinary details about a Russian assault on our election infrastructure. While there is no evidence that this assault altered the vote count, that fact should be cold comfort as we look to protect ourselves against future attacks.

One doesn't have to be an expert on cybersecurity or election technology to understand how dangerous this is. Based on my experience, as a former Director of Central Intelligence, and in service to this country under both Democratic and Republican Presidents, I am confident the Russians will be back, and that they will take what they have learned last year to attempt to inflict even more damage in future elections. In particular, their history of interfering in other nation's politics, their antipathy to the United States and Western democracies generally, and their proven ability to multiply the impact of their actions through cyberattacks should put us on the highest alert, and spur us to take all necessary actions to protect ourselves from further attack.

Of course, Moscow is not the only adversary that we have to worry about. North Korea has been implicated in the ransomware attack that locked up the computers of government agencies and businesses worldwide this May, while Al Qaeda and ISIS have a history of executing cyberattacks on foreign government websites. They too might be emboldened by Russia's actions against us last year.

This report offers important guidance on how to protect ourselves. In particular, it looks at the two most critical parts of America's election infrastructure: voting machines, which could be hacked to cast doubt on the integrity of vote tallies, or change them; and voter registration databases, which could be manipulated to block voters and cause disorder when citizens attempt to vote.

As the authors explain, much has been done to secure these systems in the last few years. But hackers have grown increasingly sophisticated in this time as well. And the state and local elections officials who are custodians of our election infrastructure often operate with highly constrained resources.

What more must be done? The key security measures detailed in this report are the right place to start: replace paperless electronic machines, upgrade the hardware and software that supports voter registration, and conduct post-election audits to confirm the results.

These are common-sense solutions that will increase security and public confidence in the integrity of our system. Importantly, they will do so without interfering with the right of any eligible citizen to participate in the choice of who will govern the nation.

Sadly, as polarization has increased in this country, even discussions of topics like how to safeguard our voting systems have broken down into partisan fighting, with each side looking for an advantage in the debate, and failing to take the steps necessary to secure our infrastructure from attack. We can no longer afford such indulgence. As has happened at key moments in our history, we face a test from outsiders who would like to harm us. We are forced to answer whether we can, once again, lay aside our differences to work together to protect the common interests of our nation.

The history of national defense shows that threats are constantly evolving. When the United States was attacked at Pearl Harbor, we took action to protect our fleet. When we were attacked on 9/11, we took action to upgrade transportation security and protect our ports and other vulnerable targets. We were attacked in 2016. The target was not ships or airplanes or buildings, but the machinery of our democracy. We will be attacked again. We must act again — or leave our democracy at risk.

INTRODUCTION

In the spring of 2017, Americans began to learn startling details of Russia's unprecedented attack on our election infrastructure. While it is important to emphasize that there is no evidence these actions changed the vote count, the attack makes clear that our country is not immune from foreign interference in our elections merely because it is the world's dominant superpower.

To a greater degree than many realize, America's election systems remain vulnerable. This is a product of old technology, inadequate systems, and a patchwork election administration model with widely varying levels of resources and skill at protecting against new-era threats. A twentieth century election system is no match for twenty-first century threats.

But we are far from helpless. This report outlines urgent steps we can take now to protect the security of the most critical elements of the U.S. election infrastructure:

- voting machines, which could be hacked to cast doubt on the integrity of vote tallies, or to even change them; and

- voter registration databases, which could be manipulated in an attempt to block voters, cause disruption, and undermine confidence when citizens vote.

The Brennan Center has studied these systems for more than a decade. Following the 2016 election, we surveyed cyber-attacks against election systems in the United States and around the world. And we conducted interviews with more than a dozen of the country's leading election officials and security experts, including officials from the Department of Homeland Security and the United States Election Assistance Commission.

This report examines the greatest vulnerabilities to the integrity of our election infrastructure, and the important steps that election officials and others have taken to protect these vulnerabilities. Above all else, we set out the measures that must be put in place as soon as possible to protect the integrity of American democracy as we prepare for elections in 2018, 2020, and beyond.

Much of the focus on Russia's attack on our election system turns on Putin and foreign policy matters. In response, sanctions and other steps may be warranted. But we can do much more to harden our election infrastructure so it is not susceptible to manipulation — by Moscow, by any other foreign power or terrorist group, or by domestic interests.

Understanding the Threat

On January 6, 2017, the Director of National Intelligence (DNI) published an extraordinary document that described a brazen attack on American sovereignty. Over the course of 14 information-packed pages, the DNI report condensed the best thinking from the FBI, CIA, and NSA about how Russia interfered in the 2016 election, in part by targeting the systems we use to run our elections.

Portions of the report read like a throwback to the Cold War, noting "Moscow's longstanding desire to undermine the US-led liberal democratic order." But what was different in 2016 is that Russia's effort

"demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations."[1]

Among other actions, the report describes the hacking of private information from political targets, including both major parties; the leaking of stolen information; and the use of media reaching U.S. audiences to spread propaganda. The report also found that "Russian intelligence obtained and maintained access to elements of multiple … state or local electoral boards, though the Department of Homeland Security assesses that the types of systems Russian actors targeted or compromised were not involved in vote tallying."

The report does not mince words about who directed this operation or its purpose:

> Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency.[2]

In the last several weeks we have learned that Russian attacks on the country's election infrastructure may have gone even further than was indicated in the DNI report. In particular, *The Intercept* reported on a leaked National Security Agency document that revealed a "months-long Russian intelligence cyber effort against" the voter registration process, "including a private sector manufacturer of devices that maintain and verify the voter rolls," as well as spear-phishing attacks against "local government organizations," and government officials "involved in the management of voter registration systems."[3] A subsequent article in *Bloomberg* stated that in Illinois "investigators found evidence that cyber intruders tried to delete or alter voter data," on the state's voter registration database and that "[i]n all, Russian hackers hit systems in a total of 39 states."[4]

Not surprisingly, American intelligence agencies have concluded that Russia will use what it learned in 2016 to meddle in future elections.[5] *Bloomberg* cited one former senior U.S. official as expressing concern "that the Russians now have three years to build on their knowledge of U.S. voting systems before the next presidential election, and there is every reason to believe they will use what they have learned in future attacks."[6] Former FBI Director James Comey has been particularly blunt, stating that "They're coming after America,"[7] and "I expect to see them back in 2018, especially in 2020."[8]

Sowing Doubt About American Democracy

Russia may have preferred Donald Trump to Hillary Clinton. But its "number one mission," as Comey told the House Intelligence Committee in March, "is to undermine the credibility of our entire democracy enterprise of this nation."[9] Russia's primary goal is to sow chaos, not necessarily to support a particular candidate.

While there is no evidence that these cyberattacks altered the vote count in 2016, all signs point to the fact that sooner or later some interest — or collection of interests — will try. As former intelligence officer Lieutenant Colonel Tony Shaffer (retired) put it in a briefing to Congress Members and staff, "anything that can be done to penetrate this system … will be done. It is just a matter of time."[10]

Moreover, as he noted in that same briefing, we should not assume we must only worry about Russia.[11] Other nations could try to attack our electoral system, whether it's an ascendant China, Iran, or North Korea, which has been linked to the ransomware attack that held hostage the computers of government agencies and businesses across the world in May of 2017.[12] The threat is not limited to nations, of course; well-organized terrorist groups such as al Qaeda or ISIS have a history of executing cyberattacks on foreign government websites and could expand their efforts.[13]

Immediate Steps Needed to Protect Our Election Infrastructure

For the past ten years, in the face of evolving cyberattacks and warnings from security experts about protecting our elections from hacking, Congress has remained strangely silent. Now, as Congressional leaders investigate Russia's interference in the 2016 election, they can take immediate, common sense actions to protect our elections from attacks in 2018 and 2020. While states and counties run our elections, the federal government and Congress have a critical role to play through funding and setting standards. All levels of government must be involved in securing our elections.

Among the most important security recommendations detailed in this report are the following:

- **Replace Antiquated Voting Machines with New, Auditable Systems.** Our election infrastructure is aging. It is time for Congress, states, and local governments to assist election officials in replacing antiquated equipment that is costly and difficult to maintain, has an increased risk of failure and crashes, and remains a significant security risk. Perhaps most importantly, Congress should act to help states and counties replace the old, paperless Direct Recording Electronic machines that are still used in 14 states, with more secure, accessible systems.

- **Conduct Audits of Paper Ballots or the Voter Verified Paper Record.** Paper records of votes have limited value against a cyberattack if they are never used to check that the software-generated total has not been hacked. Today, only 26 states require that election officials conduct post-election audits of paper records. Even in states where they are conducted, they are often insufficiently robust to ensure an election-changing software error would be found.

- **Complete a Full Assessment of Threats to Our Voter Registration Systems.** State and local governments must fully identify potential avenues for attacking voter registration systems, mapping out all of the entities that interact with that system, and implementing mitigation strategies where weaknesses are identified. The consensus among experts interviewed by the Brennan Center is that this should be done on a regular basis, but that many states are unlikely to have completed this kind of comprehensive risk assessment in the last few years, despite the fact that both registration systems and cyber threats have evolved enormously over that time.

- **Upgrade and Replace IT Infrastructure, Including Databases.** The Brennan Center estimates that 42 states are using voter registration databases that were initially created at least a decade ago. Experts interviewed by the Brennan Center agreed that many states will require upgrades to their databases and election infrastructure in the near future, and that the need is particularly great at the local level, where systems often run on discontinued software like Windows XP[14] or Windows 2000 that is more vulnerable to cyberattack because it is no longer vendor supported.

Further recommendations are discussed in more detail in the body of this report.

Critically, members of Congress and state legislatures should be talking with election officials and security experts about local needs, as they will vary by county and state. The best legislative solutions may mimic already existing bipartisan bills to address cybersecurity issues, such as the State Cyber Resiliency Act, a bill introduced in March in the Senate by Senators Warner (D) and Gardner (R) and in the House by Representatives Kilmer (D) and Comstock (R).[15] That bill requires the Federal Emergency Management Agency and DHS to work with state and local governments in administering and awarding State Cyber Resiliency Grants to protect critical infrastructure, based on the needs in those states. That is a good start. Our election infrastructure could benefit from an even more narrowly tailored program of grants that aims to provide money for the kinds of measures discussed in this report.

• • •

In May, former Director of National Intelligence James Clapper warned the Senate Judiciary Committee "If there has ever been a clarion call for vigilance and action against a threat to the very foundation of our democratic political system, this episode is it."[16] We would add that if anything can be deemed vital to our political system, it is election integrity. Indeed, election integrity is the prerequisite for democracy itself.

The Russian attacks are a powerful illustration of how the integrity of elections has become a matter of national security. Vulnerabilities in election systems can be exploited by foreign powers for their own benefit, with the potential for lasting damage to American democracy.

The threats against each system we discuss below are very real. Fortunately, they can be neutralized. In this report, we explain how.

VOTING MACHINES

Although no evidence has emerged of foreign tampering with American voting machines, the press has devoted many breathless words to the question of whether machines can be hacked.[17] The emphasis is understandable: to the average person, voting machines *are* elections. Manipulating voting machines is a concrete, easy-to-understand method for tampering with elections.

But is there an actual danger of such attacks succeeding in the United States? Based on recent experiences in other countries, the evolution of cyber-attacks over the last decade, and current vulnerabilities in our system, the answer is yes.

In fact, cyberattacks against voting systems are not just the stuff of binge-watched TV shows or movies.[18] We have seen at least two known cyberattacks on *non*-American voting systems in the last couple of decades. In 2014, Ukraine's presidential vote was targeted by cyber attackers, who deleted enough files to make the country's voting system inoperable days before the election.[19] Officials were able to restore the system from backups and the election went forward. But shortly before the results were to be announced, experts examining computers at the Ukrainian Central Election Commission discovered a virus designed to falsely declare an ultra-nationalist party as the victor with 37 percent of the vote.

A pro-Russian hacker group, CyberBerkut, claimed responsibility for the Ukrainian attacks. Experts debate whether the group is sponsored by the Kremlin.[20] One possible indication of state support, or perhaps tacit assent, is how quickly the group's exploits appeared in the Russian press. Intriguingly, the same day the virus attempting to falsify the Ukrainian vote was discovered, the Russian state-controlled Channel One incorrectly reported that the ultra-nationalist party had won with the exact same vote totals as those programmed into the virus.[21]

Russia has also been implicated in a hack against Bulgaria's Central Election Commission during a referendum and local elections in 2015.[22] While that attack did not impact the systems used to total votes, it did hit the commission's website, "which provided updates on voter turnout."[23]

Looking farther back, a hacker in South Africa attempted to steal that country's historic first democratic election in 1994 from Nelson Mandela by changing vote totals.[24] The hacker was able to access a computer remotely and add votes to the tallies of three right-wing parties, eating into the lead of Mandela's ANC party.[25] The hack was discovered, and there was a delay as the counting method was switched from electronic to manual.

It is thus not surprising that throughout the world, we have seen greater concern about how to protect voting systems from cyberattack. Most recently, the Netherlands opted to count all votes by hand in their March 2017 general election out of fear that the software used to total regional and national vote tallies was "vulnerable" to hacking.[26]

Built-in Protections Against Cyberattacks on American Voting Machines

Fortunately, the U.S. has some built-in protections against widespread attack.[27] First, the decentralization of American election administration offers perhaps the most important measure of protection. There are more than 8,000 election jurisdictions, and voters cast their ballots at about 100,000 polling places.[28] Each state or locality buys its own machines, sets its own rules for designing and counting ballots, and devises its own security measures. This means that a federal election is in many ways, thousands of separate elections, with different voting machines, ballots, rules and security measures. While there can be security downsides to such decentralization (discussed below), one clear benefit is that it is practically impossible to attack all of the nation's voting machines at a single point, as might be possible with a statewide voter registration database or campaign e-mail server.[29] Similarly, because the vast majority of voting is done on machines that are not connected to the internet, attacking them remotely is extremely difficult, in a way that might not be true for a voter registration database or a campaign's e-mail server. What this means is that the impact of any particular attack will likely be limited in geographic scope. At worst, it might impact an entire county or state, depending on how uniform the equipment, programming and processes in a particular state.

Second, particularly in the last decade, counties, states and the federal government have done much to make voting more secure. In recent years, states have taken out of service voting machines that had their own remotely-accessible wireless networks, making remote attacks much more difficult.[30]

Just as importantly, since the Help America Vote Act was passed in 2002, the Election Assistance Commission (EAC) developed standards for federal certification of voting systems, which were issued in 2005 and updated in 2015.[31] Today, 47 of 50 states rely on the EAC's federal certification program in some way.[32] This program includes much more rigorous security testing than previously existed.[33] Of course, this protection is only useful *prospectively,* for states that acquire new machines. For the many counties and states that purchased machines before the new federal standards were in place, their existence is of no benefit.

Finally, in the last few years, many jurisdictions have replaced their paperless computerized voting machines with systems that scan paper ballots filled out by voters or produce a paper trail that can be reviewed by the voter. The Brennan Center estimates that in November 2016, at least 80 percent of registered voters made selections on a paper ballot, or voted on an electronic machine that produced a paper trail.[34] This extra "software independent" record provides another important security redundancy that should act as a deterrent to attack, and should provide voters with more confidence that their votes have been counted accurately in the event there is an attack that successfully casts doubt on the integrity of the results. A public post-election audit of the voting machines can be used to confirm that the electronic record reported by the machine is correct; if systems were tampered with, a good post-election audit would let us know. This protection only applies for the 80 percent of votes cast on machines for which there is a voter verified paper record, and where good post-election audits are conducted. Unfortunately, more often than not, jurisdictions are not conducting robust post-election audits comparing paper records to software totals, so their value is frequently theoretical.

Remaining Concerns About Attacks on Voting Equipment

> *"If I were a bad guy from another country who wanted to disrupt the American system ... I think I'd concentrate on messing up the touch screen (voting) systems."*
> – Ambassador James Woolsey, former Director of the Central Intelligence Agency.[35]

Despite the security advances of the last few years, dozens of independent experts have repeatedly identified serious vulnerabilities in America's electronic voting machines.[36] One 2006 report found that commonly used machines "did not have any security mechanisms beyond what you'd find on a typical home PC."[37] Experts at the Argonne National Laboratory demonstrated in 2011 that someone with a high school education and $26 worth of parts could manipulate a voting machine that was used by more than 26 million voters in the following year's election.[38] A targeted scheme could still do significant damage to American's faith in election outcomes, and even derail the integrity of local or even national elections.

Part of the problem is that most electronic voting systems used in the United States are quite old. Forty-two states currently use voting machines that were purchased more than a decade ago.[39] This is perilously close to the end of most machines' projected lifespan, particularly machines designed and engineered in the late 1990s and early 2000s. Using aging voting equipment increases the risk of failures, vote "flipping," and crashes. Such occurrences can lead to long lines and lost votes of course, but also — in an environment where adversaries are attempting to cast doubt on the integrity of American elections — can seriously undermine voters' faith in the reliability and accuracy of our voting equipment.

Moreover, aging systems also frequently rely on unsupported software, like Windows XP or Windows 2000, which does not receive regular security patches and is more vulnerable to the latest methods of cyberattack.[40] As Jeremy Epstein of the National Science Foundation has put it, "from a security perspective, old software is riskier, because new methods of attack are constantly being developed, and older software is [more] likely to be vulnerable."[41] The ransomware attack on computer systems around the world in May 2017 illustrates the danger of using old operating systems. Hackers sponsored by North Korea's spy agency released a computer worm that locked data on victims' computers and demanded a ransom to restore access.[42] The British National Health Service was hit especially hard because it relies heavily on machines running Windows XP, which Microsoft stopped supporting in 2014.[43] In response to the crisis, security experts recommended updates with the newest security patches, but at the time there were no new patches for Windows XP.

The fact that voting machines themselves are not connected to the internet does not, by itself, fully protect us from such cyberattacks. Starting with the most limited kind of attack, experts have shown that with brief physical access to many voting machines or their removable memory cards — which contain ballot data and vote counts — a knowledgeable actor could flip the result of a local election, where the tally on a single voting machine could be extremely important.[44] Or attackers could manipulate the system to do any number of things that might shake the confidence of voters, including causing machines to crash or completely erasing vote totals. They could even change the vote tally in such an obvious way that the public would doubt all voting machines' results by, for instance, having all the votes on the machine tallied for Republican candidates in a highly Democratic polling station. In the current hyper-partisan environment, evidence of this kind of hack could lead to accusations by each side that the other is rigging the election.

Unfortunately, this kind of attack is probably easier than most people would imagine. This April, electronic poll books were stolen from the pickup truck of a poll worker during a "grocery run" shortly before a Congressional special election.[45] Physically accessing voting machines themselves is also certainly possible. Before he served in the White House Office of Science and Technology Policy, Princeton Computer Engineering Professor Ed Felten made an annual tradition of taking photos of unguarded voting machines left in polling stations in the days before Election Day.[46]

More troubling than attacks that require physical access to machines is the threat of remote attacks in which a small group of attackers could manipulate a large number of machines. While voting machines themselves are not connected to the internet, this does not make the spread of malware across machines (particularly ones used in the same city or county) impossible.[47] Just as computer viruses existed before the internet and could be spread through infected floppy disks, malware could be distributed by infected memory cards. These infected memory cards could cause the same kinds of problems discussed above, including misreporting totals and crashing machines, but on a larger scale.

A single computer can be responsible for programming hundreds of memory cards for one or more counties in a state.[48] As Professor J. Alex Halderman, Director of the University of Michigan's Center for Computer Security and Society, has noted, in several states, "many counties outsource their pre-election [memory card] programming to independent companies. In Michigan 75% of counties use just two 20 -person companies to do that programming."[49] There are no nationally mandated security requirements (for either hiring or physical protection of systems connected to ballot programming) for these vendors.[50] While some jurisdictions like New York State ban these computers from ever being connected to the internet, not all do so.[51]

Finally, state level central tabulators and election night reporting systems present another target that could seriously damage American's faith in election outcomes.[52] These central tabulators are frequently connected to the internet (just as county tabulators totaling counts from precincts may be).[53] Hacking these tabulators would probably not result in changing the official outcome of an election, as candidates and election officials would likely notice that the central tabulator outputs did not match the inputted vote totals provided by localities. Nevertheless, such hacking could seriously undermine voter confidence, if for example early reporting shows one candidate with a commanding lead that later disappears.

Solutions

While the attack scenarios discussed above paint a troubling picture, we are far from helpless against them. As discussed in greater detail below, independent security experts who have studied voting machine vulnerabilities are nearly unanimous in arguing that two of the most important things we can do to increase the security of these machines is to replace old, paperless Direct Recording Electronic ("DREs") voting machines with systems that include a "software-independent" record such as a voter verified paper ballot, and to conduct regular post-election audits that compare that record to the software totals generated by the voting machine.[54]

More generally, continuing to use antiquated voting machines perilously close to the end of their projected lifespan is a security risk. Election officials in the majority of states have told the Brennan Center that they would like to replace this equipment soon, but most do not have the money to do so.[55] Finding the

money is crucial, as is adequately funding the EAC to guide the development of the next generation of voting machines, continue publishing information about problems with existing machines, and help local election officials with their plans to purchase new equipment.

Finally, ensuring that election officials around the country have adequate resources to implement general security best practices is always of utmost importance.

Replace Antiquated Voting Machines with New, Auditable Systems

It is time for Congress, states, and local governments to assist election officials in replacing antiquated equipment that is costly and difficult to maintain, has an increased risk of failure and crashes, and that presents a significant security risk. Perhaps most importantly Congress should act to help states and counties replace the old, paperless DREs that are still used in 14 states around the country. Jurisdictions that do so must comply with the Help America Vote Act, and ensure that new voting systems do not discriminate against disabled voters, allowing them to cast votes privately and independently.[56]

At a recent public meeting of the Technical Guidelines Development Committee (TGDC) — a federal advisory committee charged with, among other things, developing federal testing guidelines for voting system security — Professor David Wagner of the committee's Working Group stated, "the number one most important thing we can do for cybersecurity would be to ensure that the voting systems are auditable." That means that "an undetected error or fault in the voting system's software," should not be "capable of causing an undetectable change in the election results," and that the voting system should "support efficient audits."[57]

For all practical purposes, given the current state of voting technology, this means that a voting system should provide a paper record that the voter has reviewed or filled out before casting her ballot on the electronic machine. The Brennan Center estimates that in 2016, at least 80 percent of registered voters made selections on a paper ballot or voted on an electronic machine that produced a paper trail.[58] This "software independent" record provides an important security redundancy that should act as a deterrent to cyberattacks and should provide voters with more confidence that their votes have been counted accurately.[59]

The Brennan Center estimates that replacing paperless machines in every jurisdiction that still uses them should cost between $130 million and $400 million. This estimate is specific to the cost of the machine itself, and does not include other items that may be included in a new voting machine contract. Many of those items (maintenance, programming, software licensing, replacement parts) will be things a jurisdiction must pay for in some amount, regardless of whether it replaces its paperless system or not; some of the items could represent new costs (e.g., training poll workers, voter education, ballot printing.) All of these costs will vary dramatically by jurisdiction.[60]

Many state and local election officials are eager to replace their antiquated systems, but have failed to convince legislatures of the urgency of doing so.[61] A time limited offer from Congress to cover even a fraction of the costs to replace these systems is likely to go a long way toward pushing states with paperless voting machines to finally replace them with equipment that makes auditing possible and relatively easy.

Conduct Audits of Paper Ballots or the Voter Verified Paper Record

Of course, paper records of votes have limited value against a cyberattack if they are never used to check that the software-generated vote total has not been hacked. Today, only 26 states require that election officials conduct post-election audits of paper records.[62] In general, these states require officials to compare a random sample of paper ballots with voting machine totals to confirm that machines are accurately counting votes. Unfortunately, as several experts have noted, even in states where they are conducted, audits are often insufficiently robust to ensure that an election-changing software error would be found.[63] Requiring post-election audits in every state, and ensuring they sample a sufficient number of ballots, is critical to catching and preventing a hack or software error from changing the results of an election. Putting post-election auditing in place requires establishing processes and allocating funding. Unless audits are mandated for federal contests, it may also require changes to state law.[64]

These post-election audits are critical not only for catching election-changing hacks, but also reassuring the public in the integrity of final vote totals. No matter what kind of attack, real or imagined, post-election audits can assure voters they can have confidence in the final results. They are an essential tool for restoring trust in the system.

Support the Election Assistance Commission

Since 2005, the EAC has performed critical functions that help increase the reliability of our voting machines. Among other things, it sets standards and provides guidance for electoral systems on criteria like performance and security. It certifies testing laboratories that ensure that equipment actually meets those standards, and manages a quality monitoring program to track, collect and share information about reported system problems. Forty-seven states have laws or rules that require them to rely on the EAC's standards, testing or certification programs when purchasing equipment.[65] In 2016, the FBI and Department of Homeland Security worked with the EAC to share information on hacking threats; former FBI Director Comey told the Senate Judiciary Committee, "That's one of the most important things we can do is equip them with the information to make their systems tighter."[66]

Despite the agency's crucial role in ensuring the integrity of elections, some members of Congress have repeatedly and recently introduced legislation to abolish the EAC.[67] But the drive to eliminate the agency is difficult to understand in the context of the size of the federal budget. With a budget of between eight and ten million dollars a year, the EAC's costs comprise a tiny sliver of federal spending. Yet eliminating the EAC's testing, certification, and monitoring programs would create an unnecessary national security risk. Rather than abolish the agency, Congress should ensure that it has adequate resources to pursue its vital mission. The EAC can guide the development of the next generation of voting machines, continue publishing information about problems with existing machines, and help local election officials with their plans to purchase new equipment.[68]

Adopt General Security Best Practices

Many of the security problems facing election systems are similar to those facing other large distributed systems, for which there are already well established security protocols. The most important of these are discussed in a document prepared by members of the Election Verification Network in response to an invitation from the Chairman of the Election Assistance Commission in the summer of 2016.[69] While the vast majority of election officials should be aware of these best practices, more resources would help ensure that they are fully implemented.

Congressional Role in Safeguarding Elections

Under the American system, states and counties are in charge of running elections. But Congress has an important supporting role to play to ensure that federal contests are fair, accessible, and secure. It can do so by providing resources and setting standards and guidelines for federal elections.

Here are three key steps Congress should take immediately to safeguard federal elections:

1. Provide grants to replace antiquated and insecure voting machines (especially paperless DREs)*;
2. Mandate robust post-election audits for federal contests, or at the very least charge a federal agency with establishing guidelines for such audits;
3. Create a grant program to fund:
    a. Threat analyses and security improvements for state and local voter registration database systems, and other essential election systems;
    b. Upgrades and replacement of critical IT infrastructure, including voter databases;
    c. Contingency, response and resiliency planning; and
    d. Ongoing cybersecurity programs, including for maintenance and updates.

*All replacement systems should satisfy HAVA's requirement to allow voters with disabilities to vote privately and independently.

VOTER REGISTRATION DATABASES

In every state except North Dakota, eligible citizens must be registered in order to vote. Under the Help America Vote Act (HAVA), passed by Congress in 2002, states are required to create and maintain statewide databases to serve as the central source of voter registration information. Despite the federal directive, state databases are subject to differing rules and use differing technologies.[70]

These databases have nothing to do with vote tallying. Rather, they tell election officials who may vote, listing the names of registered voters along with identifying information and other characteristics such as party affiliation. This means that an attack on a database will not alter voting machine counts or election night reporting systems, but they it could disrupt the orderly staging of elections and target particular groups of voters for mischief.

As with cyber threats against voting machines, the decentralization and diversity of databases can have security benefits: it makes it far less likely that database problems — whether caused intentionally or inadvertently — will impact the entire nation. The other side of the coin, though, is that the security of databases can vary greatly from one locale to the next. Some local systems may be especially vulnerable.

In securing voter registration databases, we do not need to move backwards, reversing the technology advances of the last 15 years. Rather, we need to upgrade, modernize and be smarter about how we protect this technology.

Built-in Protections Against Cyberattacks On Registration Systems

The public nature of registration lists is itself a critical security protection. Voting machines present a security challenge because of the importance our country places on the secret ballot. Because an individual has the right to keep her vote secret, it becomes more difficult to know if her vote was changed absent a "software independent" record such as a paper ballot that can be used to double check the software total. By contrast, voter registration lists are public. The parties, candidates, election officials and even voters themselves can review the voter registration lists to ensure there have been no illegitimate changes.[71]

A massive and improper manipulation of the lists is likely to be caught before, and certainly during or after an election. While the discovery of such a breach could no doubt undermine confidence in the system and potentially cause serious administrative challenges at the polls if not corrected by Election Day, there are also steps that could be taken on and after Election Day to ensure that legitimate voters can cast a ballot that will be counted. Most importantly, anyone who attempts to vote in an election must be given, at the very least, a "provisional ballot," even if the registration database indicates there is some reason they are not entitled to vote. That provisional ballot can and should be counted if the reason for the problem was manipulation of the database. In a worst case scenario, where there is evidence that a manipulation of the voter rolls might have impacted an election outcome, an election could be re-run.

Of course, ideally, there will be no breach of the database. Several election officials have informed the Brennan Center that their states have been able to use state IT security experts to harden their systems

against attack in the last decade, and some have also consulted with their state National Guard services and the FBI.[72] More recently, in 2016, the Department of Homeland Security offered assistance to local elections officials to address cyber intrusions during the run-up to the 2016 elections, including a "computer hygiene" screening that scanned election agency computers and networks for malware and vulnerabilities.[73] At least 33 states and 36 counties took advantage of the agency's offer of assistance and services.[74] And in January, 2017, DHS designated electoral systems, including voter registration databases, as "critical infrastructure," paving the way for more information sharing on vulnerabilities and DHS prioritization of election officials' requests for help.[75] In addition, DHS and the FBI have shared knowledge about the tactics hackers use against databases to inform their efforts to "make their systems tighter."[76]

Finally and importantly, in the event of a breach of a voter registration system that results in some sort of manipulation of the list, there are several redundancies within every state that should allow election officials to quickly recreate their lists, or use back up lists, so that no legitimate voter will be prevented from casting a ballot, or having their votes counted. Critically, within each state, there are both state and county lists that can be used to buttress each other in the event of a breach. At the same time, virtually every state makes a nightly, offline copy of the statewide registration database that can be used to recreate lists in the event of a breach.[77] EAC Commissioner Matt Masterson and Dr. Neil Jenkins of DHS both noted in interviews with the Brennan Center that, even before the breaches of 2016, state contingency plans for database breaches or failures were already robust.[78]

Reasons for Concern About Foreign Attacks on Registration Databases

The full extent of Russia's attempts to infiltrate state voter registration systems is not yet known. A series of news reports this year have revealed progressively more information showing the attacks to be far more pervasive than was known before the election.[79] As of the writing of this report, *Bloomberg* has reported the most far-ranging account of the attacks: that Russian agents accessed election systems in 39 states, though that number has been disputed.[80] Despite direct and repeated warnings from the Obama White House to the Kremlin about the attacks, hackers affiliated with Russia's military intelligence continued attempting to access the computers of 122 election officials until shortly before Election Day.[81]

In at least one state, Illinois, the cyber intruders tried to alter or delete records in the statewide voter registration database; they failed, but it may have been a practice run for a more aggressive attack down the line.[82] Hackers were able to access publicly-available voter files in Illinois for nearly three weeks before being detected, and the system was shut down for 10 days to address the problem.[83] Their attempts to change or delete files were blocked. And in Arizona, malware was installed on the computer of a county election official who opened an e-mail attachment.[84] That malware gave hackers access to the official's username and password, which could have been used to access a county version of the voting registration system.[85]

The Russians also attacked private vendors working for election agencies in the hopes of stealing credentials that would help them access election systems themselves. In June of 2017, *The Intercept* detailed the findings of an NSA report, which recounted a cyber-attack by Russian military intelligence

against a voter registration software company and election offices just days before the 2016 election. According to the NSA report, Russian government hackers appear to have used "data obtained from that operation to ... launch a voter registration-themed spear-phishing campaign targeting U.S. local government organizations."[86]

Not every instance of a hacker accessing a database constitutes an attempt to disrupt an election. American officials say that hackers are constantly probing state systems — both elections systems and others — sometimes hoping to steal information about individuals on government lists. "The fact someone passes by, or runs a quick test on the database and doesn't get through, that happens every day with every major database," noted Colorado Secretary of State Wayne Williams.[87]

While this is certainly true, it is also true that if a determined state actor or terrorist group was able to gain access and control of a statewide voter registration database, it would have several ways of threatening the integrity of an election in that state. As is often noted in cybersecurity circles, "a defender has to get it right every time, while an attacker only has to succeed once."[88]

Perhaps the biggest hacking threat against voter registration systems is one where hackers manipulate the databases themselves, as the Russians attempted to in Illinois last year.[89] Attackers could try to interfere with the ability of voters to cast ballots by deleting them from lists of registered voters, marking them as felons prohibited from voting, or changing party affiliation to keep them from voting in their party's primary. These obstacles could be targeted to likely voters for one side or the other through data on demographics, address, and party affiliation. If there are no back up lists, these methods could cause problems on Election Day, forcing scores of voters to cast provisional ballots, leading to long lines, undermining faith in the fairness of an election, and creating a major administrative headache to accurately count votes after the polls closed.

Another concern is related to changing addresses for existing names on the databases, or adding entirely new (and fictitious) names and addresses to cast fraudulent votes by mail. Both attacks would necessarily be limited in nature if they were to avoid detection, but they could still do significant damage to confidence in the system. In the first instance, hackers could steal votes by changing the address on file for a large number of voters and ordering absentee ballots to vote as they choose.[90] It might remain undiscovered until those voters tried to cast their ballots on Election Day and found that votes were already recorded for them. In 2012, hackers submitted computer requests for thousands of absentee ballots in Florida, but the activity was discovered.[91] Election officials would have a way of addressing this kind of attack retroactively. They could reject absentee ballots associated with forged addresses, and make sure to count provisional ballots cast by people who had their addresses improperly changed.

In the second instance, attackers could add entirely new names and addresses and request absentee ballots for those addresses. Here, merely having the "eyes" of legitimate voters on their own registration information is not enough to catch the problem. For this reason, regular and random sampling of the database to check that registered voters and addresses are real is important.

Given intelligence officials' conclusion that Russian interference is designed to weaken the public's faith in the integrity of the election process, it may be even more likely that hackers simply try to keep

databases from working.[92] They could delete whole databases[93] or use "denial of service" attacks to make systems crash on or slightly before Election Day, hampering poll workers' ability to sign voters in. This could drastically increase long lines and make voting substantially more difficult. The resulting irregularities could lead to a widespread sense that the election was rigged or otherwise illegitimate.

This is not far-fetched. There are accusations that foreign hackers targeted the British government's voter registration site with a denial of service attack on June 7, 2016, the last day citizens could register before the June 23 "Brexit" referendum. It is unclear what caused the website to become temporarily inaccessible, but a report issued by the House of Commons Public Accounts Select Committee included the possibility that the crash "may have been caused by a DDOS [distributed denial of service] attack using botnets."[94]

In addition to attacks on the integrity of voter registration systems, some have argued that foreign interests may want personal information from voter databases as part of a broader campaign of election influence that includes stealing and strategically leaking information to harm a candidate or party, as the Russians did with the hack of the Democratic National Committee.[95] Damaging information can be included in ads that are custom designed for a specific demographic, and stolen personal information would allow those ads to be micro-targeted to that demographic through emails or social media. And even without any further election-related use of voter registration information, the violation of voters' privacy can be used to harm them in other ways and can in and of itself undermine confidence in the election system.

Solutions

Given the centrality of the voter registration system to elections in nearly every state, it is surprising that there has been "very little research ... on the security and integrity of state voter registration databases ... certainly nowhere near the amount of research that has focused on the security of other components of the American election infrastructure."[96] Going forward, election professionals and independent researchers in the election field would do well to devote more resources to studying the security of state voter registries.

In the meantime, based on a review of existing literature as well as interviews with election officials in several states, the Brennan Center is able to make several observations about immediate steps that should be taken to increase the security of voter registration systems around the country. Most importantly, to the extent they have not already done so, every state should complete a thorough audit and threat analysis of their registration system, hardening the system against attack, making it more difficult for breaches to succeed, and easier to catch breaches if and when they happen. In many states, hardening the system against attack will involve upgrading and replacing antiquated IT infrastructure, including database software and operating systems.

Of course, no system can be made completely secure. If there are determined actors there will eventually be breaches against the system. States should be reviewing and updating contingency plans in the event of a successful breach that interferes with the integrity of the system, correct data is available and recoverable when needed, and eligible citizens will not be prevented from registering or voting.

The solutions offered below are quite specific, but not all states and localities will share exactly the same needs. There is no comprehensive study of voter registration systems, making it nearly impossible to pinpoint which states and localities could benefit most from a particular security measure. Congress has an important role to play in securing the nation's voter registration. It may want to follow the example of the bipartisan State Cyber Resiliency Act, a bill introduced in March in the Senate by Senators Warner (D) and Gardner (R) and in the House by Representatives Kilmer (D) and Comstock (R).[97] That bill requires the Federal Emergency Management Agency and DHS to work with state and local governments in administering and awarding State Cyber Resiliency Grants to protect critical infrastructure. Grants can support projects that will enhance "preparation, response and resiliency of computer networks," "implementing a process of continuous cyber security vulnerability assessments," adopting cybersecurity best practices, and mitigating talent gaps in the government workforce. States and localities could benefit from a more narrowly tailored program of grants that aims to provide money for the same sort of measures, more focused on securing the voter registration system.

Voter registration systems differ significantly from state to state. This provides both advantages and disadvantages from a security perspective. Because each one is different (and in most cases not built from a common software base), an attacker must develop many different methods of manipulating different kinds of databases. On the other hand, because there is so much diversity, it is far more difficult to obtain cost advantages and economies of scale by building common defenses.

Harden Systems by Updating Threat Awareness

Experts we spoke to agreed that the first step that state and local governments should take in securing voter registration systems is to regularly and fully identify the potential avenues for attack, mapping out all of the systems and entities that interact with a particular voter registration system, and developing and implementing mitigation strategies where weaknesses are identified.[98]

This may be more difficult than it sounds. A statewide registration database is constantly changing, as new information (related to registration status, voting history, and the like) comes in from voters (on line and through paper applications inputted into the system), and from a host of government actors including county election officials who keep their own lists (and may be using insecure work stations to access and update information), Departments of Motor Vehicles, social service agencies, and other states (for purposes of cross-checking duplicate registrations), among many others. As Merle King, executive director for the Center for Election Systems at Kennesaw State University in Georgia put it, "Each interface or vector ... carries inherent risk...there may be hundreds of interfaces between the [voter registration] system and county election offices and thousands of interfaces between the [voter registration] system and poll books at polling locations. Knowing the nature of these interfaces, the function they serve, the quantity and the roles and responsibilities for defining and using these interfaces is key to understanding the threat(s)."[99] In addition to understanding what must be protected, those working on security must also understand where the vulnerabilities to cyberattack are. What are the potential threats for each kind of interaction with the system? What the implications might be if a breach happened at any particular point? What can be done to identify successful intrusions and mitigate against them? And how to best prevent breach and manipulation in the first place?

There was a consensus among the experts interviewed that many states are unlikely to have completed this kind of risk assessment and audit in the last few years, despite the fact that both registration systems and cyber threats have evolved enormously over that time.[100] The cost of completing a threat assessment is likely to be manageable. The State of Ohio recently completed a full security scan of its registration system for approximately $25,000.[101] The State of Virginia also recently finished a partial threat assessment of its registration system that it considered to be the "most critical" at a cost of $40,000. Edgardo Cortes, Commissioner of the Virigina Department of Elections, estimates his department would need $80,000 annually to conduct a comprehensive" threat assessment or audit, though he notes that "[t]his is just the actual audits — costs for mitigating any identified issues would be separate."[102]

The data from Ohio and Virginia suggest that the national cost of performing such audits could come in between $1 million and $5 million annually (with the important caveat that if weaknesses were identified, there could be additional costs for increased security).[103]

The Department of Homeland Security may be able to help state and local jurisdictions carry out threat assessments and implement needed mitigation, but ultimately such a project must be led by the election offices that know and use the registration system. While states and local governments will bear the majority of the cost for such assessments, Congress has a role to play too. Targeted grants through DHS to support threat analyses and audits would encourage these urgently needed projects in all 50 states.

Upgrade and Replace IT Infrastructure, Including Databases

For many jurisdictions the single most important step in hardening may be a wholesale upgrade of the databases and the software and hardware supporting them. Based on individual state HAVA reports, annual reports from secretaries of state, and subsequent contracts for new systems, the Brennan Center estimates that 42 states are using voter registration databases that were initially created at least a decade ago.[104]

In that time, cyber threats have advanced enormously. "These systems weren't designed with [current cyber threats] in mind," according to Edgardo Cortes, Commissioner for the Virginia Department of Elections. If anything, the use of outdated databases and operating systems present even more challenges than those associated with using old voting machines. As Marc Burris, Chief Information officer of the North Carolina State Board of Elections put it, at least the oldest voting machines in the United States were actually "designed for a longer shelf life. That's not true of many of the database systems we are using today."

At least five states have recently put out requests for information, quotation or proposal to replace or upgrade their systems, while the State of Virginia is already in the process of making major upgrades on its own.[105]

Experts interviewed by the Brennan Center believed that many more states would likely require such upgrades in the near future.[106] At the same time, regular security maintenance — for things like security patches, software upgrades and licensing fees — may become more costly, as most states have exhausted

the federal HAVA funds that helped them create the federally mandated databases in the first place.[107] Congress mandated the creation of these computerized statewide voter registration databases, noted Matt Damschroder, Assistant Secretary of State and Chief of Staff to the Ohio Secretary of State. While he views the creation of those systems as ultimately beneficial to elections, he noted that the failure to pay for ongoing upkeep of these systems has left election officials in a bind. "Election administration always plays second fiddle to other things that [state and local] funders need to fund."

The need for updates or replacement of IT infrastructure and software may be even greater at the local level, where systems often run on discontinued software like Windows XP or Windows 2000 that is more vulnerable to cyberattack because it is no longer vendor supported. This is particularly troubling because smaller jurisdictions frequently have little or no IT support of their own.[108] "At the state level, you are generally going to have more resources and higher levels of sophistication," noted Damschroder. Local election official are likely to have "far fewer resources," to protect against attacks.[109]

Adopt General Security Best Practices and Employ Contingency Plans

As with voting machines, employing general best practices for protecting against cyberattack will be useful in defending voter registration databases. This includes limiting employees' access to registration database as much as possible, securing work stations used by employees to access databases, and programming databases to run frequent, automated scans of registration activity to monitor for and alert election officials to potentially fraudulent or abnormal activity, such as a high volume of traffic or oddly timed traffic. A more complete list of such practices can be found in the Brennan Center's white paper, *Voting System Security and Reliability Risks*.[110] It also includes conducting regular random audits of the registration lists themselves, to ensure that registered voters are real people and that mailing address for voters are legitimate.

But of course, no system can be made completely secure. For this reason, it is also essential to ensure that election officials can recover records quickly, and that citizens can continue to effectively register and vote, in the event of a successful breach.

The basics of such contingency planning should be well known to most election officials. Among other things, staff should be trained on cyber-security best practices and a written contingency plan. Contingency plans should clearly inform employees of the steps they must take in various defined scenarios, like the loss of registration data, detection of the addition of unauthorized data, or the detection of a hacker's probe. Training should include practice drills or "war games." To protect against data being manipulated or deleted, backups should be made regularly, on removable media isolated from internet connections as well as on paper.[111] Contingency plans should cover when and how to restore databases from backups, and staff should practice executing data recovery. Neil Jenkins of DHS noted that when it came to contingency planning, election officials had the kind of mentality he had seen in the military and homeland security, describing election officials as "robust planners... [they know] they have one day to do it and do it right."[112]

DHS and the EAC may be able to help state and local jurisdictions refine their security protocols and contingency plans by sharing best practices from around the country. But having good plans is only the

first step. As many election officials noted, ensuring that good security plans are actually executed can often be the most expensive part of the plan. "People have considerably underestimated the amount of resources needed to keep these databases secure," explains Edgardo Cortes. Douglas Kellner, Co-Chair of the New York State Board of elections adds that even with the best security protocol, getting resources for "enforcing and maintaining [them] is [often] the biggest challenge."[113]

Ensure Election Day Failsafe

Perhaps the most important thing to know about the security of voter registration databases and election integrity is that as long as states and local jurisdictions keep backups, including paper copies of their registration lists, no manipulation of state computer registration databases should ever prevent legitimate voters from casting a ballot, or having their votes counted.

In a worst case scenario, election officials may not realize there are problems with the voter registration list until Election Day. But even then, voters whose names are not on the list should be provided with provisional ballots that can be counted later, when the compromised registration list is reconstructed with the backups.

Officials should run tests to ensure that they are able to revert to the database as stored in an offline electronic backup in case of an attack. In jurisdictions where electronic poll books are used, the system should include paper backups of poll books, as well.

Electronic Poll Books

Electronic pollbooks (also known as e-pollbooks) are electronic versions of the voter rolls that can be used to process voters at the polls instead of using paper-based lists. Use of e-pollbooks has spread dramatically over the last decade. While only a handful of jurisdictions used them in 2006, today, 34 states and the District of Columbia use e-pollbooks for at least some portion of voting.[114]

The Presidential Commission on Election Administration recommended the use of e-pollbooks "for greater accuracy and efficiency."[115] Among the many benefits of e-pollbooks is that they can make it much easier to set up "vote centers" during early voting or on Election Day. Vote centers are "an alternative to traditional, neighborhood-based precincts." Anyone in a particular jurisdiction can vote there, regardless of where in the jurisdiction they live.[116] If a county uses multiple vote centers, the e-pollbooks can automatically sync up during the day to ensure that once someone has voted in a particular location, they can't vote in another on the same day.

While e-pollbooks have many election administration advantages, they also pose additional security challenges. As with registration databases, someone who gained control over these pollbooks could delete names from the pollbooks, mark individuals as felons prohibited from voting or as eligible citizens who already voted, or change peoples' party affiliation to keep them from voting in a party primary. While anyone impacted by such changes would have the right to ask for a provisional ballot, which could be counted after a hack or manipulation was discovered, such an attack could greatly undercut confidence in the election system, and figuring out which provisional ballots to count would be a logistical headache for election officials and poll workers.

Unlike voting machines, there are currently no national security standards for electronic poll books. Of the 34 states using electronic pollbooks, only 13 have statewide procedures or certification requirements, or certify systems statewide, according to NCSL.[117] That leaves close to two dozen states that do not have statewide procedures or certification requirements for these systems.

While there was no unanimity from election officials we spoke to on whether it was a good idea, states might benefit from the creation of voluntary federal guidelines for the security (and usability and accessibility) of e-pollbooks. Publication of such guidelines by the Election Assistance Commission is clearly permitted (if not required) under Section 222 of the Help America Vote Act.[118]

Whether the EAC does so or not, we recommend that states and localities considering the purchase of e-pollbooks work with the EAC as they develop their own test reports and standards before buying such systems. Several states, including Ohio, Virginia, California, and Indiana have collaborated with the EAC on such efforts in recent months.[119]

E-pollbooks make it simpler for election officials to run flexible, efficient elections that make voting easier. The Brennan Center encourages their use, but also urges all states using them to have paper backups of poll books ready for use in the event of their malfunction, whether due to glitches, poll worker error, or a denial of service attack.

A Note About Federal, State and Local Cost Sharing

The steps we recommend in this paper cost relatively little, certainly in comparison to the potentially damaging consequences the nation could suffer if we fail to take them. Even the most expensive step, replacing the most insecure and antiquated voting machines, is an additional expense in the tens of millions of dollars, not the hundreds of millions or billions the country routinely spends for other aspects of national security.

Unfortunately, at the moment, legislators do not appear to feel nearly enough urgency about taking these needed precautions. Part of the problem, as always in American elections, is that control is divided among federal, state and local governments. Too often, state and local governments have been slow to invest in election infrastructure, even in the face of warnings from election officials and security experts that the consequences of failing to act could be dire.[120]

Meanwhile, issues of election administration generally receive almost no attention from Congress, except when it adds new mandates in the form of laws like the Help America Vote Act. Many of these mandates address important and necessary matters, like replacing failed voting equipment or making it easier for military and overseas voters to cast a ballot that will be counted.[121] But they come with additional long term costs for which states and localities have not budgeted.

Of course, states and localities want to run elections where all eligible voters cast ballots that will be counted. And Congress has an obligation to ensure that federal contests are run with security and integrity. It is for these reasons that many of the recommendations in this report follow a formula: Congress should provide the states and localities with a time-limited offer of a partial grant in exchange for a commitment to complete the needed security step (replacing voting equipment, conducting meaningful post-election audits of federal elections, completing new threat analyses and audits for voter registration systems). We believe that this formula will provide states and localities with the urgency and resources needed to finally take these overdue measures.

CONCLUSION

The intelligence community's assessment is that Russia will continue to escalate its interference in our democracy, and other foreign powers or terrorist groups may become even bolder in the years to come. Complacency is not an option. There are weak points in our election system's armor that need to be shored up immediately. Voting machines and voter registration databases, in particular, represent two of the most critical systems to protect from attack.

Unfortunately, election law and policy has become intensely polarized, like so many contemporary issues. Both parties are too often guilty of using debates around election systems and their integrity to seek electoral advantage or whip up their base. Indeed, it is almost impossible to imagine today's Congress mustering bipartisan support for reform legislation like that seen for the Federal Election Campaign Act of 1974 or the Help America Vote Act of 2002.

But this is a national security issue too. So we should heed the wise words of Senate Foreign Relations Chairman Arthur Vandenberg who, in leading bipartisan efforts to craft defenses against the threat posed by the post-war Soviet Union, declared we must stop "partisan politics at the water's edge."[122] National security is no place for partisan squabbling. We all share the goal of protecting American democracy against foreign interference, and we must come together to safeguard the integrity of our elections.

The reforms we propose will make our elections safer and protect public confidence in their legitimacy. And time is of the essence. Implementing reforms does not happen quickly; the process must get started in order to be complete in time for the next federal elections.

We must recognize that we live in a world where foreign interests are vying for power on the world stage by trying to shape American politics, or even attempting to create doubts that democracy really works. Against that backdrop, it is clear that strengthening election security is essential to protecting our national security.

ENDNOTES

1 *Assessing Russian Activities and Intentions in Recent U.S. Elections*, ICA 2017-01D, Office of the Director of National Intelligence, 2017, ii.

2 Ibid.

3 Matthew Cole et al., "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election," *The Intercept*, June 5, 2017, https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.

4 Michael Riley and Jordan Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known," *Bloomberg*, June 13, 2017, https://www.bloomberg.com/politics/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.

5 *Assessing Russian Activities and Intentions in Recent U.S. Elections*, Office of the Director of National Intelligence, iii.

6 Riley and Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known,.

7 *Open Hearing of the Senate Intelligence Committee*, 115th Cong. (2017) (statement of James Comey, Former Director of the Federal Bureau of Investigation).

8 *Oversight of the Federal Bureau of Investigation, Before the Senate Committee on the Judiciary*, 115th Cong. (2017) (statement of James Comey, Director of the Federal Bureau of Investigation). Comey made similar remarks in House testimony, saying, "they'll be [back] in 2020, they may be back in 2018 and one of the lessons they may draw from this is that they were successful because they introduced chaos and division and discord and sewed doubt about the nature of this amazing country of ours and our democratic process." *Open Hearing on Russian Active Measures Investigation, Before the House Intelligence Committee*, 115th Cong. (2017) (statement of James Comey, Director of the Federal Bureau of Investigation).

9 *Open Hearing on Russian Active Measures Investigation, Before the House Intelligence Committee* (statement of James Comey, Director of the Federal Bureau of Investigation).

10 Lt. Col. Tony Shaffer, Senior Fellow at the London Center for Policy Research and former intelligence officer, "Congressional Briefing: Strengthening Election Cybersecurity," Moderated by Karen Greenberg, May 15, 2015, https://youtu.be/Mlqv952Rb4w.

11 Ibid.

12 Ellen Nakashima, "The NSA has linked the WannaCry computer worm to North Korea," *Washington Post*, June 14, 2017, https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.91dec512312b.

13 Kim Sengupta, "Isis-linked hackers attack NHS websites to show gruesome Syrian civil war images," *The Independent*, February 7, 2017, http://www.independent.co.uk/news/uk/crime/isis-islamist-hackers-nhs-websites-cyber-attack-syrian-civil-war-images-islamic-state-a7567236.html; Vasudevan Sridharan, "Al-Qaeda hacks Indian railways website urging Muslims to take up jihad," *International Business Times*,

March 2, 2016, http://www.ibtimes.co.uk/al-qaeda-hacks-indian-railways-website-urging-muslims-take-jihad-1547051; Joseph Marks, "ISIL aims to launch cyberattacks on U.S.," *Politico*, December 29, 2015, http://www.politico.com/story/2015/12/isil-terrorism-cyber-attacks-217179.

14 Microsoft recently announced that it is "releasing a new patch for Windows XP, a product it no longer formally supports, out of concern for state-sponsored cyberattacks." Ali Breland, "Microsoft releases new update citing concern over state-sponsored attacks," *The Hill*, June 13, 2017, http://thehill.com/policy/technology/337646-microsoft-releases-unusual-update-out-of-nation-state-concerns.

15 "S.516 - State Cyber Resiliency Act," accessed June 7, 2017, https://www.congress.gov/bill/115th-congress/senate-bill/516/related-bills; "H.R.1344 - State Cyber Resiliency Act," accessed June 7, 2017, https://www.congress.gov/bill/115th-congress/house-bill/1344?r=2.

16 Washington Post Staff, "Full Transcript: Sally Yates and James Clapper Testify on Russian Election Interference," *Washington Post*, May 8, 2017, https://www.washingtonpost.com/news/post-politics/wp/2017/05/08/full-transcript-sally-yates-and-james-clapper-testify-on-russian-election-interference/?utm_term=.897cd34f213f.

17 See NPR Staff, "After DNC Hack, Cybersecurity Experts Worry About Old Machines, Vote Tampering," *NPR*, August 20, 2016, http://www.npr.org/sections/alltechconsidered/2016/08/20/490544887/after-dnc-hack-cybersecurity-experts-worry-about-old-machines-vote-tampering; Laurie Segall, "Just how secure are electronic voting machines?," *CNN*, August 9, 2016, http://money.cnn.com/2016/08/09/technology/voting-machine-hack-election/; Brian Barrett, "America's Electronic Voting Machines Are Scarily Easy Targets," *Wired*, August 2, 2016, https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election/.

18 *House of Cards*, "Season 5," Directed by Daniel Minahan, et al., Netflix, May 30, 2017; *Scandal*, "Defiance," Directed by Tom Verica, Written by Shonda Rhimes and Peter Noah, ABC, November 29, 2012.

19 Mark Clayton, "Ukraine election narrowly avoided 'wanton destruction' from hackers," *Christian Science Monitor*, June 17, 2014, http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video.

20 Jeff Stone, "Meet CyberBerkut, The Pro-Russian Hackers Waging Anonymous-Style Cyberwarfare Against Ukraine," *International Business Times*, December 17, 2015, http://www.ibtimes.com/meet-cyberberkut-pro-russian-hackers-waging-anonymous-style-cyberwarfare-against-2228902.

21 Clayton, "Ukraine election narrowly avoided 'wanton destruction' from hackers."

22 Oren Dorell, "Russia Engineered Election Hacks and Meddling in Europe," *USA Today*, January 9, 2017, https://www.usatoday.com/story/news/world/2017/01/09/russia-engineered-election-hacks-europe/96216556/.

23 "Huge Attack on Bulgaria Election Authorities 'Not to Affect Vote Count'," *Novinite.com (Sofia News Agency)*, October 27, 2015, http://www.novinite.com/articles/171533/Huge+Hack+Attack+on+Bulgaria+Election+Authorities+%27Not+to+Affect+Vote+Count%27.

24 John Leyden, "Hacker almost derailed Mandela election in South Africa," *The Register*, October 27, 2010, https://www.theregister.co.uk/2010/10/27/sa_election_hack/.

25 Martin Plaut, "Book says hacker tried to stop Mandela coming to power," *BBC*, October 26, 2010, http://www.bbc.com/news/world-africa-11630092.

26 "Dutch will count all election ballots by hand to thwart hacking," *The Guardian*, February 1, 2017, https://www.theguardian.com/world/2017/feb/02/dutch-will-count-all-election-ballots-by-hand-to-thwart-cyber-hacking.

27 FBI Director Comey said, voting is "very, very hard to hack into because it is so clunky and dispersed." See Elizabeth Weise, "Could the U.S. election be hacked?," *USA Today*, October 10, 2016, https://www.usatoday.com/story/tech/news/2016/10/10/could-us-election-hacked/91866334/.

28 *The 2014 EAC Election Administration and Voting Survey Comprehensive Report*, U.S. Election Assistance Commission, 2015, 259-260, https://www.eac.gov/assets/1/1/2014_EAC_EAVS_Comprehensive_Report_508_Compliant.pdf.

29 See *Protecting the 2016 Elections from Cyber and Voting Machine Attacks, Hearing 4, Before the House Committee on Space, Science & Technology*, 114th Cong. (2016) (statement of Dr. Dan S. Wallach, Professor of Computer Science at Rice University), https://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-114-SY-WState-DWallach-20160913.pdf; Sanger and Savage, "Sowing Doubt Is Seen as Prime Danger in Hacking Voting System."

30 Jenna Portnoy, "Va. Board of Elections votes to decertify some voting machines," *The Washington Post*, April 14, 2015, https://www.washingtonpost.com/local/virginia-politics/va-board-of-elections-votes-to-decertify-some-voting-machines/2015/04/14/46bce444-e2a6-11e4-81ea-0649268f729e_story.html.

31 *U.S. Election Assistance Commission*, "EAC Updates Federal Voting System Guidelines," news release, March 31, 2015, https://www.eac.gov/assets/1/28/EAC%20Updates%20Federal%20Voting%20System%20Guidelines-News-Release-FINAL-3-31-15-website.pdf.

32 See *Protecting the 2016 Elections from Cyber and Voting Machine Attacks, Before the House Committee on Space, Science & Technology*, 114th Cong. (2016) (statement of Dr. Charles H. Romine, Director of the Information Technology Laboratory at the Department of Commerce's National Institute of Standards and Technology), http://democrats.science.house.gov/sites/democrats.science.house.gov/files/documents/Romine%20Testimony.pdf; Brian Hancock, Merle S. King, and Matthew Masterson, *Infrastructure Requirements for the Testing and Certification of Election Systems*, Bowen Center for Public Affairs, 2015, http://bowencenterforpublicaffairs.org/wp-content/uploads/2015/05/Infrastructure-Requirements-for-the-Testing-and-Certification-of-Election-Systems_FINAL.5.13.15.pdf.

33 *Protecting the 2016 Elections from Cyber and Voting Machine Attacks, Before the House Committee on Space, Science & Technology* (statement of Dr. Charles H. Romine, Director of the Information Technology Laboratory at the Department of Commerce's National Institute of Standards and Technology), https://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-114-SY-WState-CRomine-20160913.pdf.

34 *Cybersecurity: Ensuring the Integrity of the Ballot Box, Before the Committee on House Oversight and Government Reform, Subcommittee on Information Technology*, 114th Cong. (2016) (statement of Lawrence D. Norden, Deputy Director, Democracy Program, Brennan Center for Justice at NYU School of Law), https://oversight.house.gov/wp-content/uploads/2016/09/2016-09-28-Norden-NYU-Testimony.pdf.

35 "Why a Fmr. CIA Director is Worried about Voting Machines," *Fox Business* video, 1:16. November 7, 2016, http://video.foxbusiness.com/v/5199936869001/?#sp=show-clips.

36 Ben Wofford, "How to Hack an Election in 7 Minutes," *Politico*, August 5, 2016, http://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144.

37 Ibid; Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine*, Princeton University, 2006, https://css.csail.mit.edu/6.858/2012/readings/accuvote-ts.pdf.

38 Victoria Collier, "How to Rig an Election," *Harper's*, November 2012, http://harpers.org/archive/2012/11/how-to-rig-an-election/?single=1.

39 Lawrence Norden and Christopher Famighetti, *America's Voting Machines at Risk*, Brennan Center for Justice, 2015, 9, https://www.brennancenter.org/publication/americas-voting-machines-risk. Note that since the publication of this report, Rhode Island has purchased new voting machines. "Rhode Island buys 590 new voting machines," *The Associated Press*, July 21, 2016, https://apnews.com/25d780c61bbb44f78d7ed55c76a3b189.

40 Merle King (Executive Director, Center for Election Systems, Kennesaw State University), in phone discussion with Lawrence Norden, February 5, 2015; Joe Rozell (Director of Elections, Oakland County, Michigan), in phone discussion with Lawrence Norden, February 24, 2015; Neal Kelley (Registrar of Voting, Orange County, California), in phone discussion with Lawrence Norden, February 2, 2015; Ryan Macias (Voting Systems Analyst, Office of the Secretary of State, California), in phone discussion with Lawrence Norden, March 13, 2015; Joseph Mansky (Elections Manager, Ramsey County, Minnesota), in phone discussion with Lawrence Norden, April 30, 2015; Sherry Poland (Director of Elections, Hamilton County, Ohio), in phone discussion with Lawrence Norden, February 18, 2015; Garth Fell (Elections and Recording Manager, Snohomish County, Washington), in phone discussion with Lawrence Norden, April 30, 2015; Jeremy Epstein (Deputy Division Director, National Science Foundation), email message to Lawrence Norden, May 30, 2015.

41 Jeremy Epstein (Deputy Division Director, National Science Foundation), email message to Lawrence Norden.

42 Ellen Nakashima, "The NSA has linked the WannaCry computer worm to North Korea."

43 Brian Barrett, "If You Still Use Windows XP, Prepare For the Worst," *Wired*, May 14, 2017, https://www.wired.com/2017/05/still-use-windows-xp-prepare-worst/.

44 *Security Assessment of WinVote Voting Equipment for Department of Elections*, Virginia Information Technologies Agency Commonwealth Security and Risk Management, April 14, 2015, http://www.elections.virginia.gov/WebDocs/VotingEquipReport/WINVote-final.pdf.

45 Christopher Wallace, "New details emerge in theft of Ga. voting machines," *Fox News*, April 18, 2017, http://www.foxnews.com/politics/2017/04/18/new-details-emerge-in-theft-ga-voting-machines.html.

46 Ed Felten, "E-Voting Links for Election Day," *Freedom to Tinker*, November 2, 2010, https://freedom-to-tinker.com/2010/11/02/e-voting-links-election-day/.

47 See *Protecting the 2016 Elections from Cyber and Voting Machine Attacks, Hearing 4, Before the House Committee on Space, Science & Technology*, (statement of Dr. Dan S. Wallach, Professor of Computer Science at Rice University) (explaining that malware can be spread to machines not connected to the internet, as the Stuxnet malware was when introduced into nuclear facilities in Iran.).

48 See Jesse B. Staniforth, "How Easy Would It Be to Rig the Next Election?," *ThinkProgress*, May 1, 2017, https://thinkprogress.org/how-easy-would-it-be-to-rig-the-next-election-819326cbbbd (quoting computer science expert Matt Bernhard saying, "These are small businesses with little to no operational security oversight on the part of the government ... So any breach would be hard to detect").

49 Matt Bernhard and J. Alex Halderman, "Recount 2016: An Uninvited Security Audit of the U.S. Presidential Election," (presentation, University of Michigan, December 28, 2016), https://media.ccc.de/v/33c3-8074-recount_2016_an_uninvited_security_audit_of_the_u_s_presidential_election#video&t=19.

50 Jeremy Epstein notes that the use of outside vendors to program memory cards could introduce another vulnerability, depending on the security protocol in place. It is possible "that the localities email the ballot information to the outsourced company, which sets up the configuration and emails the files back for loading onto the voting machines. If [this happens], then those files could be manipulated in transit to change their behavior. Additionally, this [would imply] that although the voting machines themselves may be offline, they're getting removable media from a machine that's connected to the internet." Jeremy Epstein (Deputy Division Director, National Science Foundation), email message to Lawrence Norden.

51 N.Y. Comp. Codes R. & Regs. tit. 9, § 6210.5(b).

52 Staniforth, "How Easy Would It Be to Rig the Next Election?." (quoting Mark Graff, former chief information security officer for NASDAQ, saying that "a much more attractive approach would be to attack those machines that are aggregating the votes...").

53 Ibid, ("aggregation systems, [Graff] notes, handle significantly larger numbers of votes than precinct machines, and are likelier to be connected to the internet."); Douglas Kellner (Co-Chair, State Board of Elections, New York), email message to Lawrence Norden, May 11, 2017; Karen Hobart Flynn and Pamela Smith, "Why voting systems must be as secure as the U.S. power grid," *Reuters*, August 17, 2016, http://www.reuters.com/article/us-security-internet-voting-commentary-idUSKCN10S08G.

54 Feldman, Halderman, and Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine*, 14; Tadayoshi Kohno et al., *Analysis of an Electronic Voting System*, IEEE, 2004, 21, http://avirubin.com/vote.pdf.

55 Norden and Famighetti, *America's Voting Machines at Risk*, 5.

56 Help America Vote Act, 52 U.S.C.A. § 21081 (2015).

57 "U.S. Election Assistance Commission Technical Guidelines Development Committee, Meeting February 13-14, 2017: Day 1, Part 3," *National Institute of Standards and Technology* video, 2:06, February 13, 2017, https://www.nist.gov/news-events/events/2017/02/tgdc-meeting-february-13-14-2017.

58 See "Voting System Security and Reliability Risks", *Brennan Center for Justice*, 2016, https://www.brennancenter.org/sites/default/files/analysis/Fact_Sheet_Voting_System_Security.pdf.

59 *Cybersecurity: Ensuring the Integrity of the Ballot Box, Before the Committee on House Oversight and Government Reform, Subcommittee on Information Technology, United States House of Representatives*, (statement of Lawrence D. Norden, Deputy Director, Democracy Program, Brennan Center for Justice at NYU School of Law).

60 For more details see Lawrence Norden and Christopher Famighetti, *Estimate for the Cost of Replacing Paperless, Computerized Voting Machines*, Brennan Center for Justice, 2017, https://www.brennancenter.org/sites/default/files/analysis/New_Machines_Cost_Across_Paperless_Jurisdictions%20%282%29.pdf.

61 Lawrence Norden and Christopher Famighetti, "Now Is the Time to Replace Our Decrepit Voting Machines," *Slate*, November 17, 2016, http://www.slate.com/articles/technology/future_tense/2016/11/now_is_the_time_to_fix_our_old_voting_machines.html; Michael R. Wickline, "Bill to buy poll gear falls short," *Arkansas Online*, March 23, 2017, http://www.arkansasonline.com/news/2017/mar/23/bill-to-buy-poll-gear-falls-short-20170-1/?f=news-arkansas; David Saleh

Rauf, "States Scramble for Funding to Upgrade Aging Voting Machines," *US News*, March 12, 2017, https://www.usnews.com/news/best-states/texas/articles/2017-03-12/states-scramble-for-funding-to-upgrade-aging-voting-machines.

62 *Cybersecurity: Ensuring the Integrity of the Ballot Box, Before the Committee on House Oversight and Government Reform, Subcommittee on Information Technology, United States House of Representatives*, (statement of Lawrence D. Norden, Deputy Director, Democracy Program, Brennan Center for Justice at NYU School of Law).

63 Philip B. Stark, "Risk-limiting Postelection Audits: Conservative P-values from Common Probability Inequalities," IEEE Transactions on Information Forensics and Security 4.4, (2009), 1013, http://ai2-s2-pdfs.s3.amazonaws.com/c6f0/4c884e5382d0ecbea9239b83224982dc6411.pdf.; *Cybersecurity: Ensuring the Integrity of the Ballot Box, Before the Committee on House Oversight and Government Reform, Subcommittee on Information Technology, United States House of Representatives*, (statement of Lawrence D. Norden, Deputy Director, Democracy Program, Brennan Center for Justice at NYU School of Law); Ronald L. Rivest and John P. Wack, "On the notion of "software independence" in voting systems," Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 366, (2008), 3, https://pdfs.semanticscholar.org/37a3/9c83f6c77bdafb3012a3b70aab8070298a25.pdf.

64 For instance, in Virginia, the state law on audits includes the following requirement "No audit conducted pursuant to this section shall commence until after the election has been certified and the period to initiate a recount has expired… [a]n audit shall have no effect on the election results." 2017 Va. Acts Ch. 367.

65 See *Protecting the 2016 Elections from Cyber and Voting Machine Attacks, Committee on Science, Space and Technology, United States House of Representatives*, (statement of Charles H. Romine, Ph.D., Director, Information Technology Laboratory, National Institute of Standards and Technology, United States Department of Commerce); Hancock, King, and Masterson, *Infrastructure Requirements for the Testing and Certification of Election Systems.*

66 *Oversight of the Federal Bureau of Investigation, Before the Senate Committee on the Judiciary*, (statement of James Comey, Director of the Federal Bureau of Investigation).

67 Russell Berman, "The Federal Voting Agency Republicans Want to Kill," *The Atlantic*, February 13, 2017, https://www.theatlantic.com/politics/archive/2017/02/election-assistance-commission-republicans-congress/516462/.

68 Norden and Famighetti, *America's Voting Machines at Risk*, 7.

69 U.S. Election Assistance Commission, *Election Verification Network 2016 Short-Term Recommendations*, January 28, 2016, https://www.eac.gov/assets/1/28/EVN%20Top%20Ten%20v7.pdf.

70 *Assorted Rolls: Statewide Voter Registration Databases Under HAVA*, electionline.org, 2005, http://www.pewtrusts.org/~/media/legacy/uploadedfiles/wwwpewtrustsorg/news/press_releases/election_reform/electionline0605pdf.pdf.

71 47 states allow voters to check their registration online. The Brennan Center verified this number by checking each state's registration lookup website. Voters are unable to check their voter registration status in Maine, Mississippi, and Wyoming. "Check Your Registration! 50 State Guide. Don't let dirty tricks block your vote.," *DailyKos*, September 19, 2016, https://www.dailykos.com/story/2016/9/19/1572027/-Check-Your-Registration-50-State-Guide-Don-t-let-dirty-tricks-block-your-vote

72 Douglas Kellner, "Elections as Critical Infrastructure," (presentation, New York Board of Elections, March 17, 2017), http://electionverification.org/wp-content/uploads/2017/01/Kellner-cybersecurity-20170317.pptx; Douglas Kellner (Co-Chair, State Board of Elections, New York), email message to Lawrence Norden; Marian Schneider (Deputy Secretary for Elections and Administration, Department of State, Pennsylvania), in phone discussion with Lawrence Norden, May 5, 2017; Edgardo Cortes (Commissioner, Department of Elections, Virginia), in phone discussion with Lawrence Norden, May 24, 2017; Matthew Masterson (Commissioner, U.S. Election Assistance Commission), in phone discussion with Lawrence Norden, June 2, 2017; Matt Damschroder (Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio), in phone discussion with Lawrence Norden May 25, 2017.

73 David E. Sanger and Charlie Savage, "Sowing Doubt Is Seen as Prime Danger in Hacking Voting System," *New York Times*, September 14, 2016, https://www.nytimes.com/2016/09/15/us/politics/sowing-doubt-is-seen-as-prime-danger-in-hacking-voting-system.html.

74 "NASS Reports on State Officials Findings RE: 2016 U.S. Elections," *National Association of Secretaries of State*, March 21, 2017, http://www.essvote.com/blog/98.

75 Chase Gunter, "DHS vague on rules for election aid, say states," *FCW*, February 14, 2017, https://fcw.com/articles/2017/02/14/what-does-dhs-mean-by-critical.aspx; The Department of Homeland Security, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," news release, January 6, 2017, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

76 *Oversight of the Federal Bureau of Investigation, Before the Senate Committee on the Judiciary*, (statement of James Comey, Director of the Federal Bureau of Investigation).

77 Matthew Masterson (Commissioner, U.S. Election Assistance Commission), in phone discussion with Lawrence Norden; Neil Jenkins (Chief of Policy and Planning, Department of Homeland Security, National Protection and Programs Directorate, Office of Cybersecurity & Communications), in phone discussion with Lawrence Norden, June 13, 2017.

78 Ibid.

79 Ibid.

80 Riley and Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known." However, on June 21, 2017, during a hearing of cybersecurity officials before the Senate Intelligence Committee, a Department of Homeland Security official said that only 21 states "were potentially targeted by Russian government-linked cyber actors." Tal Kopan, "DHS officials: 21 states potentially targeted by Russia hackers pre-election," *CNN*, June 21, 2017, http://www.cnn.com/2017/06/21/politics/russia-hacking-hearing-states-targeted/index.html.

81 Ibid.

82 Ibid.

83 Ibid; "Illinois Elections Board Offers More Information on Hacking Incident," *Illinois Public Radio*, May 4, 2017, http://news.wsiu.org/post/illinois-elections-board-offers-more-information-hacking-incident.

84 Jeff Pegues, "After hack, Arizona working to keep its elections database secure," *CBS News*, October 13, 2016, http://www.cbsnews.com/news/after-hack-arizona-working-to-keep-its-elections-database-secure/.

85 Wesley Bruer and Evan Perez, "Officials: Hackers breach election systems in Illinois, Arizona," *CNN*, August 30, 2016, http://www.cnn.com/2016/08/29/politics/hackers-breach-illinois-arizona-election-systems/.

86 Cole et al., "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election."

87 Eric Geller and Daniel Samuelsohn, "More than 20 states have faced major election hacking attempts, DHS says," *Politico*, September 30, 2016, http://www.politico.com/story/2016/09/states-major-election-hacking-228978.

88 Kevin Poulsen, "Surprise! America Already Has a Manhattan Project for Developing Cyber Attacks," *Wired*, February 18, 2015, https://www.wired.com/2015/02/americas-cyber-espionage-project-isnt-defense-waging-war/.

89 Riley and Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known." "If you can steal the data, you can change it," said Art Gilliland, a cyber security executive. Eric Chemi and Mark Fahey, "Assessing the threat of Russia hacking the US election," *CNBC*, October 11, 2016, http://www.cnbc.com/2016/10/11/russian-hackers-may-try-to-disrupt-us-elections.html.

90 "If you can impersonate a person, you can request a ballot," according to voting security expert Pamela Smith of Verified Voting. Cory Bennett, "Election fraud feared as hackers target voter records," *The Hill*, May 2, 2016, http://thehill.com/policy/cybersecurity/278231-election-fraud-feared-as-hackers-target-voter-records; Mark Potter, "Cyberattack on Florida election is first known case in US, experts say," *NBC News*, March 18, 2013, http://investigations.nbcnews.com/_news/2013/03/18/17314818-cyberattack-on-florida-election-is-first-known-case-in-us-experts-say.

91 Potter, "Cyberattack on Florida election is first known case in US, experts say." The scheme turned out to have been executed by a congressional staffer seeking an advantage in voter outreach. Patricia Mazzei, "Ex-aide to Miami Rep. Joe Garcia to head to jail in absentee-ballot case," *Miami Herald*, October 20, 2013, http://www.miamiherald.com/news/local/community/miami-dade/article1956526.html.

92 Sanger and Savage, "Sowing Doubt Is Seen as Prime Danger in Hacking Voting System."

93 The master copy of the registration database should never be online. But even deletion of a working copy that interfaced with other portals on a particular day would be extremely disruptive.

94 Josh Lowe, "Foreign Powers May Have Hacked Brexit Voter Registration Site, British MPs Say," *Newsweek*, April 12, 2017, http://www.newsweek.com/brexit-voter-registration-site-hack-russia-germany-macron-france-582697.

95 Kate Brannen, "Connecting the Dots: Political Microtargeting and the Russia Investigation," *Just Security*, May 19, 2017, https://www.justsecurity.org/41199/connecting-dots-political-microtargeting-russia-investigation-cambridge-analytica/.

96 Michael Alvarez, "How secure are state voter registration databases?," *Election Updates*, October 12, 2016, http://electionupdates.caltech.edu/2016/10/12/how-secure-are-state-voter-registration-databases/.

97 State Cyber Resiliency Act - S.516; State Cyber Resiliency Act - H.R. 1344.

98 Merle King (Executive Director, Center for Election Systems, Kennesaw State University), in phone discussion with Lawrence Norden; Marc Burris (IT Director and CIO, State Board of Elections, North Carolina), in phone discussion with Lawrence Norden, May 22, 2017; Edgardo Cortes (Commissioner, Department of Elections, Virginia), in phone discussion with Lawrence Norden; Stuart Holmes (Voting

Information System Manager, Washington Secretary of State), in phone discussion with Lawrence Norden, June 8, 2017.

99 Merle King (Executive Director, Center for Election Systems, Kennesaw State University), in phone discussion with Lawrence Norden.

100 Merle King (Executive Director, Center for Election Systems, Kennesaw State University), in phone discussion with Lawrence Norden; Marc Burris (IT Director and CIO, State Board of Elections, North Carolina), in phone discussion with Lawrence Norden; Matt Damschroder (Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio), in phone discussion with Lawrence Norden; Edgardo Cortes (Commissioner, Department of Elections, Virginia), in phone discussion with Lawrence Norden; Stuart Holmes (Voting Information System Manager, Washington Secretary of State), in phone discussion with Lawrence Norden, June 8, 2017.

101 Matt Damschroder, (Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio), in phone discussion with Lawrence Norden.

102 Edgardo Cortes (Commissioner, Department of Elections, Virginia), email message to Lawrence Norden, June 20, 2017.

103 Ohio and Virginia are the seventh and twelfth largest states respectively. If we assume that Ohio and Virginia's costs for conducting a full assessment represent the low and high end for conducting such assessments (in fact for much smaller states the cost would likely be less) the cost for all 50 states would range somewhere between. "List of U.S. states and territories by population," *Wikipedia*, https://en.wikipedia.org/wiki/List_of_U.S._states_and_territories_by_population.

104 The Brennan Center arrived at this figure by examining information made available by the U.S. Election Assistance Commission and by individual states. That information principally included HAVA grant reports, HAVA extension requests, state HAVA reports, state contracts for new systems, and Secretaries of State annual reports. Based on a review conducted on May 23, 2017, we estimate that 42 states implemented their voter registration database by the end of 2006. Those 42 states are: Alaska, Arizona, Arkansas, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Minnesota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Utah, Vermont, Washington, West Virginia, and Wisconsin.

105 Texas Secretary of State, *Purchase Order*, (Austin, Texas, 2014), http://www.sos.state.tx.us/about/procurement/2017-invoices/307-4-00455.pdf; State of New Jersey Department of the Treasury, *T-2840 Hosting, Maintenance, Support for the NJ Statewide Voter Registration System*, (Trenton, NJ, 2012), http://www.state.nj.us/treasury/purchase/noa/contracts/t2840_13-x-22355.shtml; Arizona Department of State, Office of the Secretary of State, *Bid Solicitation: ADSPO17-00007130*, (Phoenix, Arizona, 2017), https://procure.az.gov/bso/external/bidDetail.sdo?bidId=ADSPO17-00007130&parentUrl=activeBids; Washington State Office of the Secretary of State, *ITPS Work Request*, (Olympia, WA, 2017), https://www.sos.wa.gov/_assets/office/RFQQ%2017-08%20Work_Request.pdf; S.B. 2170, 100th Gen. Assemb., Reg. Sess. (Ill. 2017).

106 Edgardo Cortes (Commissioner, Virginia Department of Elections), in phone discussion with Lawrence Norden; Merle King (Executive Director, Center for Election Systems, Kennesaw State University), in phone discussion with Lawrence Norden; Matt Damschroder, (Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio), in phone discussion with Lawrence Norden; Marc Burris,

(Chief Information Officer, State Board of Elections, North Carolina), in phone discussion with Lawrence Norden; Stuart Holmes (Voting Information System Manager, Washington Secretary of State), in phone discussion with Lawrence Norden, June 8, 2017.

107 The U.S. Election Assistance Commission, *Annual Grant Expenditure Report Fiscal Year 2015*, 2016, 2, https://www.eac.gov/assets/1/28/Final%20FY%202015%20Grants%20Report.pdf.

108 Norden and Famighetti, *America's Voting Machines at Risk*, 39; Merle King (Executive Director, Center for Election Systems, Kennesaw State University), in phone discussion with Lawrence Norden; Edgardo Cortes (Commissioner, Department of Elections, Virginia), in phone discussion with Lawrence Norden; Matt Damschroder (Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio), in phone discussion with Lawrence Norden.

109 Matt Damschroder, (Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio), in phone discussion with Lawrence Norden.

110 "Voting System Security and Reliability Risks," Brennan Center for Justice.

111 Ibid, 3-4.

112 Neil Jenkins (Chief of Policy and Planning, Department of Homeland Security, National Protection and Programs Directorate, Office of Cybersecurity & Communications), in phone discussion with Lawrence Norden.

113 Douglas Kellner (Co-Chair, State Board of Elections, New York), email message to Lawrence Norden.

114 "VRM in the States: Electronic Poll-books," last modified February 6, 2017, Brennan Center for Justice, http://www.brennancenter.org/analysis/vrm-states-electronic-poll-books.

115 Presidential Commission on Election Administration, "Presidential Commission on Election Administration Presents Recommendations to President Obama," news release, January 22, 2014, http://web.mit.edu/supportthevoter/www/2014/01/22/presidential-commission-on-election-administration-presents-recommendations-to-president-obama/.

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

117 "VRM in the States: Electronic Poll-books," Brennan Center for Justice.

118 52 U.S.C.A. § 20962.

119 Matthew Masterson (Commissioner, U.S. Election Assistance Commission), email message to Lawrence Norden, June 12, 2017.

120 Norden and Famighetti, *America's Voting Machines at Risk*, 8–20.

121 52 U.S.C.A. § 20902, 20982.

122 Senate Historical Office, "Featured Bio: Senator Arthur Vandenberg," *United States Senate*, https://www.senate.gov/artandhistory/history/common/generic/Featured_Bio_Vandenberg.htm.

QUESTIONS FOR THE RECORD

Dr. Samuel Liles, Acting Director of Cyber Division, Office of Intelligence and Analysis

And

Jeanette Manfra, Acting Director of Undersecretary, National Protection and Programs Directorate

U.S. Department of Homeland Security

QUESTIONS FOR THE RECORD FROM SENATOR WARNER

1. **Question: Please provide a description of the full scope of Russian attempts to interfere in the 2016 elections in the United States by hacking into, or attempting to hack into state and local election systems, including, but not limited to, voter registration databases, voting machines, voting-related computer networks or secretaries of state and other election officials' networks.**

   Response: The Office of Intelligence and Analysis (I&A) published a comprehensive intelligence report in early October 2016, largely based on suspected malicious tactics and infrastructure, that cataloged suspicious activity we observed directed at state government election infrastructure across the country. While not a definitive source in identifying individual activity attributed to Russian government cyber actors, it established that Internet-connected election-related networks, including websites, in 21 states were potentially targeted by Russian government cyber actors. A copy of this product has been previously provided to this committee.

   This cyber activity was characterized by similarities in the tactics employed, the infrastructure used by malicious cyber actors, and the victimized networks themselves. The activity was also, concurrent with the Russian government's compromise and leaks of e-mails from U.S. political figures and institutions. The capabilities and tactics were largely in the form of spear-phishing individual e-mail accounts and attempts to exploit database vulnerabilities using Structure Query Language (SQL) injection.

   Supported by classified reporting we've refined our understanding of individual targeted networks, but the scale and scope noted in that October 2016 report still generally characterizes our observations: a small number of networks were successfully compromised, there were a larger number of states where attempts to compromise networks were unsuccessful, and there were an even greater number of states where only preparatory activity like scanning was observed.

2. **Please identify the 21 states potentially targeted by Russian government cyber actors referenced in the prepared testimony and provide any additional relevant information related to localities and the nature of the targeted networks.**

Response: While not a definitive source in identifying individual activity attributed to Russian government cyber actors, the Department of Homeland Security (DHS) is aware of Internet-connected election-related networks, including websites, in at least 21 states that were potentially targeted by Russian government cyber actors. Although we've refined our understanding of individual targeted networks, supported by classified reporting, our observations include: a small number of networks were successfully compromised, there were a larger number of states where attempts to compromise networks were unsuccessful, and there were an even greater number of states where only preparatory activity like scanning was observed.

Entities impacted by malicious cyber activity engage with the Department of Homeland Security on a voluntary basis. Our success requires strong partnerships built on trust and confidentiality. By identifying affected entities, we not only make it less likely that the affected entity will continue to engage with DHS, but also it becomes less likely that other entities are willing to share information with the government.

It's important to note, however, that by working with affected entities, the Department has been able to share information with thousands of election officials about the nature of the threat. Facing the threat of cyber-enabled operations by a foreign government during the 2016 elections, the Department of Homeland Security conducted unprecedented outreach and provided cybersecurity assistance to state and local election officials. Through numerous efforts before and after Election Day, DHS and our interagency partners have declassified and publicly shared significant information related to the Russian malicious cyber activity. These steps have been critical to protecting our elections, enhancing awareness among election officials, and educating the American public.

QUESTIONS FOR THE RECORD FROM SENATOR WYDEN

3. **According to the January 2017 Intelligence Community Assessment (ICA), DHS assessed that "the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying." DHS's prepared testimony stated that it is "likely that cyber manipulation of U.S. election systems intended to change the outcome of a national election would be detected."**

   What level of confidence does DHS have in its assessment included in the ICA?

   Response: DHS I&A has moderate confidence in the ICA that "the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying," a judgement based on our analysis of observed Russian cyber operations, the Intelligence Community's ability to detect such activity, and the Department's insight into the various components of U.S. election infrastructure.

4. **Does DHS assess that it would be likely that cyber manipulation of U.S. election systems intended to change the outcome of a state or local election would be detected?**

   Response: Beyond our separate assessment of the access Russia developed into U.S. election infrastructure in 2016- accesses that did not provide the direct ability to alter vote tallies - DHS I&A has high confidence that it is likely that cyber manipulation of US election infrastructure intended to change the outcome of a national election would be detected. We have not made an assessment of state-wide or local elections.

   Does DHS assess that it would be likely that cyber manipulation of U.S. election systems would be detected, regardless of whether it was intended to, or did, change the outcome of any U.S. election?

   Response: Multiple checks and redundancies in U.S. election infrastructure—including diversity of systems, non-Internet connected voting machines, pre-election testing, and processes for media, campaign, and election officials to check, audit, and validate results—make it likely that cyber manipulation of U.S. election systems, at a scale and scope intended to change the outcome of a national election, would be detected. There is always the possibility that individual or isolated cyber intrusions into U.S. election infrastructure could go undetected, especially at local levels, but a broad coordinated effort is likely to be detected.

5. **To what extent does the ability to detect cyber manipulation of vote tallying depend on whether the manipulation is conducted through remote access of internet-connected systems or through other means?**

   Response: The risk to U.S. computer-enabled election infrastructure varies from county to county, between types of devices used, and among processes used by polling stations. These factors, among others, introduce resilience in the overall system but also introduce numerous variables into our ability to detect cyber manipulation of U.S. election infrastructure, whether remotely or through physical access to a system. We judge that physical access to a system, in most cases, would be more difficult to detect than remote access, but an accurate assessment of our ability to detect an individual cyber intrusion into U.S. election infrastructure is system-specific, especially against vote tallying systems that are diverse and generally non-Internet connected.

6. **DHS's prepared testimony describes a range of services available to state and local election officials. Do these services address possible vulnerabilities related to vote tallying systems, particularly systems that are not internet-facing? If not, why not? If so, to what extent did state and local election officials avail themselves of these services?**

Response: The Department of Homeland Security (DHS) has shared information with election officials, including indicators of compromise, technical data, and best practices that assist officials with addressing threats and vulnerabilities related to election infrastructure that is not Internet-facing.

Additionally, DHS offers risk and vulnerability assessments. These assessments are more thorough and done on-site by DHS cybersecurity experts. They typically require two to three weeks and include a wide range of vulnerability testing services, focused on both internal and external systems. When DHS conducts these assessments, we provide a full report of vulnerabilities and recommended mitigations following the testing. Due to available resources, these assessments are available on a limited basis.

Generally, DHS is authorized, upon request, to provide cybersecurity functions including technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to cyber threat indicators, defensive measures, cybersecurity risks, and incidents, which may include attribution, mitigation, and remediation. As we continue to work with election officials, we may identify opportunities to provide additional services.

7. **DHS testimony during the hearing included the following: "We are currently engaged with many vendors of [voting machine] systems to look into conducting some joint forensics with them. The vendor community is very interested in engaging with us.... Our department has not conducted forensics on specific voting machines."**

   What is the timeline for conducting joint DHS-vendor forensic examinations of voting machines?

   How broadly will those examinations be conducted? In what states will they be conducted and what percentage of voting machines will be subject to the examinations?

   What is the role of state and local election officials in this effort?

   Response: The Department of Homeland Security (DHS) continues to work with the vendor community to determine what cybersecurity services would be of interest to them, to include vulnerability testing. DHS's work with vendors and election officials is on a voluntary basis. To the extent that technical assistance is requested from vendors and resources are available, DHS will leverage its capabilities to provide assistance.

8. **Has DHS conducted any assessments of the ability of state and local authorities, technology vendors and contractors to identify and defend against sophisticated cyber attacks conducted by nation states? If so, what are those assessments?**

   Response: On September 20, 2016, the Department of Homeland Security published an intelligence assessment on Cyber Threats and Vulnerabilities to US Election Infrastructure. The assessment was published at the unclassified-for official use only level. This assessment was shared with federal stakeholders and states' election officials.

9. **The Election Assistance Commission (EAC) issues voluntary voting system guidelines. How many states adhere to these guidelines?**

   Response: The Election Assistance Commission is an independent agency. Based on discussions with the Election Assistance Commission, we understand that there are at least 41 states that use Federal standards and certification processes in some manner. For more detailed information, we respectfully defer to the EAC.

10. **Does DHS have an assessment about the value of paper voting or the risks posed by paperless electronic voting systems? If so, what is that assessment?**

    Response: Owners and operators of critical infrastructure manage risk. The Department of Homeland Security (DHS) has prioritized efforts to assist state and local election officials address cybersecurity and physical risks related to election infrastructure. DHS has not made recommendations related to how a state should or should not allow voters to cast ballots.

11. **According to an investigation by Politico, Kennesaw State University, which is responsible for all voting technology for the state of Georgia, had lax cybersecurity, which security researchers exploited to download registration records for the state's 6.7 million voters and multiple PDFs with instructions and passwords for election workers to sign in to a central server on Election Day. The report also stated that the University failed to fully correct these vulnerabilities even after it was notified.**

    Does DHS concur with the findings of the investigation?

    What actions can be taken to address the vulnerabilities identified by the investigation and what role could DHS have played, or could play in the future in addressing those vulnerabilities?

    Response: The Department of Homeland Security (DHS) is authorized, upon request, to provide cybersecurity functions including technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to cyber threat indicators, defensive measures, cybersecurity risks, and incidents, which may

include attribution, mitigation, and remediation. DHS did not receive a request for assistance in relation to the facts described in this question. As a result, DHS did not conduct an independent assessment related to the findings of the investigation.

12. In August 2016, DHS announced it had created an Election Infrastructure Cybersecurity Working Group. Who is on this Working Group and does it include cybersecurity experts with a technology background?

Response: The Department has had significant engagement efforts with election infrastructure stakeholders since last year. The Election Infrastructure Cybersecurity Working Group announced in August 2016 included officials from the Department of Homeland Security, the Department of Justice, the Federal Bureau of Investigation, the National Institute of Standards and Technology, the National Association of Secretaries of State, The Election Assistance Commission, and the National Association of State Election Directors. This group was leveraged prior to the 2016 election to share information and consider options.

The Secretary formally established the Election Infrastructure Subsector in January 2017. As the Sector-Specific Agency the Department will provide overall coordination guidance on election infrastructure matters to subsector stakeholders. As part of this process, the establishment of the Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) is nearing completion. The EIS GCC will be a representative council with the mission of focusing on sector-specific strategies and planning. This will include development of information protocols and establishment of key working groups, among other priorities, once chartered and meeting regularly. As part of the GCC establishment, we recently assembled a cyber-focused Election Infrastructure Operational Working Group (OWG) comprised of key Federal, state and local partners. The purpose of the group is to jointly develop information sharing requirements and protocols using the expertise of key state election officials and the Multi-State Information Sharing Analysis Center (MS-ISAC). This OWG has membership from across the Department of Homeland Security's National Protection and Programs Directorate, Election Assistance Commission, National Association of Secretaries of State, National Association of State Election Directors, key county officials, and the MS-ISAC. The OWG includes many cybersecurity experts with technology backgrounds and will continue to refine requirements as it matures.

13. To what extent should secretaries of state and other election officials receive security clearances necessary to obtain cyber threat information from the federal government?

What level of clearance is required?

Response: The Department of Homeland Security is committed to providing security clearances to state chief election officials and select election support personnel, on a "need to know" basis. While the predominance of information sharing will be at the unclassified level, working with cleared election officials allows the sharing of relevant classified information with appropriate officials at the state level. We have initiated the security clearance process for state chief elections officials, using the existing clearance request process for state and local government officials.

With thousands of election jurisdictions across the country, it would be a significant challenge to provide a security clearance to every official with election responsibilities. While security clearances allow officials to better understand the classified context around cyber threat information, it is important to note that the Department is committed to declassifying as much information as possible in order to allow for the broadest dissemination and network protection. For instance, prior to the 2016 election, while information related to sources and methods remained classified, to the extent possible, the federal government declassified certain information related to attribution as well as technical cyber threat information that election officials could use to defend their networks.

○