EMERY CELLI BRINCKERHOFF & ABADY LLP

RICHARD D. EMERY
ANDREW G. CELLI, JR.
MATTHEW D. BRINCKERHOFF
JONATHAN S. ABADY
EARL S. WARD
ILANN M. MAAZEL
HAL R. LIEBERMAN
DANIEL J. KORNSTEIN
O. ANDREW F. WILSON
ELIZABETH S. SAYLOR
DEBRA L. GREENBERGER
ZOE SALZMAN
SAM SHAPIRO
ALISON FRICK
DAVID LEBOWITZ
HAYLEY HOROWITZ
DOUGLAS E. LIEB
ALANNA SMALL
JESSICA CLARKE

ATTORNEYS AT LAW
600 FIFTH AVENUE AT ROCKEFELLER CENTER
10TH FLOOR
NEW YORK, NEW YORK 10020

TELEPHONE
(212) 763-5000
FACSIMILE
(212) 763-5001
WEB ADDRESS
www.ecbalaw.com

CHARLES J. OGLETREE, JR.
DIANE L. HOUK

December 23, 2016

***By Federal Express***

Attorney General Loretta Lynch
U.S. Department of Justice
950 Pennsylvania Ave, NW
Washington, DC 20530

*Re: Election integrity*

Dear Attorney General Lynch:

We are counsel to Jill Stein and the Stein Campaign in connection with the recounts she sought in Michigan, Pennsylvania, and Wisconsin. We write to urge the Department of Justice to launch an investigation into the integrity of our nation's election system generally, and our nation's voting machines specifically, based on the information we discovered in the course of this representation. The attempted recount process has uncovered that voting machines relied on in these states and across the country are prone to human and machine error, especially in under-resourced black and brown communities, and vulnerable to tampering and hacking. The recount also found that the states' efforts to protect their systems may be insufficient, particularly in low-income communities and communities of color. Each of these grave concerns warrants federal intervention.

**The Vulnerability and Unreliability of Our Voting Apparatus**

The need for the recounts in these states was prompted in part by the vulnerability of the voting machines relied on in these three states. There are at least two types of vulnerabilities: susceptibility to malicious interference and poor performance. These reliability issues are magnified in communities of color, which the United States Commission on Civil Rights has found are often more likely to have their votes miscounted or tossed out than predominately white communities.

Voting Machines Errors and Election Day Problems

Optical scan machines are also prone to commit errors. The experts testified that optical scan machines do not consistently read light marks, misread hesitation marks, and give erroneous results if ballots are incorrectly fed into the machine, among other issues. When those machines are antiquated and not maintained appropriately, their performance is worsened. Add human error to that failing technology, and the result is *thousands* of votes not being counted.

The 2016 Election was marked by serious problems, which was only fully revealed during the recount process. The halted recount in Michigan provides powerful evidence of these problems. The recount was completed in 2,725 of Michigan's 7,786 precincts, or just about one-third. In those precincts alone, over 1,600 votes were discovered never to have been counted. Thousands more would have been discovered had the recount continued. Every one of those voters was disenfranchised by machines that misread their ballots. The recount also revealed the terrible state of Michigan's election machinery. Machines throughout the state are over ten years old and many could not stand up to the stress of another Election Day.

Michigan's unusual election results also raise red flags regarding potential interference with election results. A very large number of votes cast contained no vote for president, which is known as the "undervote." This year, 1.5% of the total vote in the state was an undervote—75,335 undervotes—a figure substantially higher than in recent presidential election years. The number of undervotes also dwarfs the 10,704 margin between the top two candidates.

In Michigan, over 87 voting machines broke on Election Day in Detroit alone, according to city election officials. The City Clerk Janice Winfrey reported that, although she had requested newer models from the state, they were never provided. Detroit, a city with heavy concentrations of minorities and low-income families, was effectively denied the opportunity to benefit from more reliable voting machines.

Another problem that particularly plagued low-income areas in Michigan was the mishandling of ballots and other essential documents. Multiple precincts in Detroit lost their poll books—the only record of whom and how many people showed up to vote. Nearly a quarter of ballots in Wayne County, which includes Detroit, were not securely handled, resulting in fewer ballots in ballot boxes than were recorded as having been issued, as well as improperly sealed and improperly transported ballot boxes. In one dramatic example, one Detroit precinct's sealed container that was supposed to hold the precinct's 307 ballots after Election Day had just 52 ballots in it when it was opened to be recounted. Again, Wayne County was not alone. Nearly 11 percent of *all* precincts statewide that were examined during the recount were afflicted with similar irregularities. And the worst cases were in some of the poorest counties. For example, problems were found in 24% of Cass County and Ionia County precincts, and in 27% of Branch County precincts. All three, along with Wayne, have per capita incomes substantially below the state median and are evidently not provided with sufficient resources to ensure that sufficient numbers of competent poll workers are hired, trained, and employed on Election Day and

thereafter to secure the votes of all Michigan citizens.[1]

In Pennsylvania, many voters who requested absentee ballots never received them in time to cast their vote. There were so many problems with absentee ballots that a Montgomery County judge ordered a four-day extension of the deadline to return them, warning that 17,000 people could be disenfranchised without an extension.[2] Voters also reported issues with DREs that appeared to inaccurately record their votes on Election Day. The "no vote" button on Sequoia AVC Advantage machines in Montgomery County remained lit even after voters attempted to press other buttons to vote for candidates. Voters feared that their votes were inaccurately counted as "no votes." Indeed, the election results for Montgomery County included 4,087 "no votes"—meaning either that 4,087 people implausibly went to their polling places only to vote for *no* candidate in *any* election, or that the machines did not work.[3]

Cyber Vulnerabilities – and the Inaccuracy of FBI Director Comey's Testimony

The optical scan and direct-recording electronic ("DRE") voting systems used throughout the country rely on computers with reprogrammable software, making them vulnerable to bugs, malware, or intentional alterations. Our nation's leading cyber-security experts have analyzed these machines and concluded that a reasonably skilled attacker can easily infect the voting machines with malware or other alterations, which can cause the machines to provide any result of the attacker's choosing. Professor Alex Halderman, the Director of the Center for Computer Security and Society at the University of Michigan, has personally hacked into several voting machines as part of a research study, including the optical scan model used in Michigan. He was able to do so within minutes. Similarly, Dr. Harri Hursti has developed a series of tests demonstrating how easily the voting results of the studied machines could be altered. These computer scientists are the opposite of luddites. They embrace electronic

[1] We are gratified to see that, as a result of the recount, Michigan is now taking some of these problems seriously. For example, it is currently auditing some of the worst performing precincts in Detroit. And the state has agreed to buy Detroit new voting machines. Unfortunately, while investigations and audits are clearly required throughout the state, the Republican legislature and State Department have focused only on heavily Democratic and minority Detroit. Irregularities were just as prevalent in heavily Republican Cass and Ionia Counties and worse in Republican stronghold Branch County, but not a word has been said condemning local election officials in those counties, and no effort has been made to audit their practices. More troublingly, Republican state officials have spun the story so that irregularities are said to result from voter fraud in heavily minority communities, rather than endemic state-wide problems due to underfunding, inadequate training and oversight, and similar non-partisan problems.

[2] *See* Laura McCrystal, *Montco Judge Extends Deadline for Absentee Ballots*, Phila. Inquirer, Nov. 4, 2016, *available at* http://www.philly.com/philly/news/politics/20161104_Montco_seeks_to_extend_deadline_for_absentee_ballots.html.

[3] *See General Election Unofficial Results*, Montgomery County, http://webapp.montcopa.org/election/2016%20General%20Election%20Result.htm (last visited Dec. 19, 2016).

tabulation of the vote but insist that we recognize computers' vulnerabilities—and thus use paper verification.

How could a cyberattack occur given FBI Director James Comey's sworn testimony to Congress that no election machines are ever connected to the internet? *See* Ex. A at 48, 63 ("Those things are not connected to the internet."). First, Director Comey's testimony is inaccurate. The administrator of the Wisconsin Elections Commission testified under oath that some voting machines connect to the internet: "[S]ome of the newer equipment [referring to voting machines] does have modems that operate using wireless Internet. And so after the polls close, then when those unofficial results are transmitted, in some cases they could be transmitted. That instantaneous transaction would be conducted over the Internet." Ex. B at 125 (transcript of testimony of M. Haas, Nov. 29, 2016). One such machine that has internet connectively, according to the vendor's own marketing materials, is the ES&S DS200, which processes optical scan ballots.[4] We understand this new ES&S DS200 model is in broad use in approximately 25 states around the country.

Second, even where the voting machine is never itself connected to the internet, each voting machine connects to other machines that *are* connected to the internet to obtain the ballot software for each election (among other reasons). The Wisconsin Elections Commission administrator testified that private vendors provide "removable media"—basically, a thumb/USB drive—with that ballot software prior to each election. Ex. B at 105-106. In Wisconsin, that removable media transfers software from computers under the control of a private vendor, and is then "inserted into the voting machine before the election." *Id.* at 106. Wisconsin has no rules requiring private vendors to protect their computers from cyberattacks. *Id.* at 105-106. Those private computers may be exceptionally vulnerable to attacks and any malware that is installed on the vendors' computer can be transferred, through the removable media, to voting machines across the state. In this way, a hack of one vulnerable machine located in a private office could propagate a devastating cyberattack far and wide, even in states where election administration is decentralized. According to elections experts, processes similar to Wisconsin's, in which electronic voting machines are programmed with software transferred from computers in government or private offices that are likely connected to the Internet, occur nationwide. No national cybersecurity standards for these computers exist.

When California and Ohio conducted comprehensive reviews of electronic voting systems, both states discovered vulnerabilities in *every* voting machine studied. For instance, 30% of Pennsylvania voters use the Election Systems & Software iVotronic (a DRE machine); the Ohio Secretary of State found easily circumventable security protections and vulnerabilities in this machine that could be exploited to introduce malware. 29% of Pennsylvania voters use the Danaher Shouptronic 1242, a DRE model that was introduced in the 1980s, has not had its security features updated in thirty years, and "lost" about 200 votes in a 2005 election in

[4] ES&S's website markets the DS200 as including a "Modem: Accumulates and transmits votes directly from the polling place." *See* http://www.essvote.com/products/13/1/digital-scan-tabulators/ds200/ (last accessed Dec. 19, 2016).

Pennsylvania.[5]

Steps that many election officials undertake to safeguard the DRE and optical scan machines against hacking, like using seals and testing the machines with a smaller deck of ballots, can be easily defeated by an attacker set on interfering with an election.

A federal district court judge in Michigan said it best: "The vulnerability of our system of voting poses the threat of a potentially devastating attack on the integrity of our election system." *Stein v. Thomas*, No. 2:16-cv-14233, slip op. at 7 (E.D. Mich. Dec. 7, 2016).

**Insufficient Checks to Ensure our Voting System's Integrity**

In light of the vulnerability to cyberattacks and the problems with our voting machines, a system of checks to ensure the accuracy of the vote is imperative. As one cyber-security expert testified, our election system must adopt the mantra of "trust but verify." Unfortunately, our verification system is inadequate for at least four discrete reasons.

First, our verification system is inadequate because too many votes are tabulated with no paper trail whatsoever. In Pennsylvania, more than 85% of voters vote on DRE machines with no paper trail. These Pennsylvanian voters cannot know whether the machines have accurately recorded their votes. Unfortunately, 15 states have no paper trail for some or all of their votes.[6] Only approximately 70% of voters nationwide have their votes recorded on some form of paper. Thankfully, Wisconsin and Michigan have paper trails for each vote,[7] which was crucial for recount efforts.

Second, even when paper records are available, too often those paper records are ignored in favor of a machine recount. "Recounting" a vote using the machine that originally counted the vote is meaningless; one expert compared it to seeking a second opinion from the same doctor. Yet that is what happened in 21 Wisconsin counties which chose to use machine recounts in whole or part, ignoring the best evidence of the voter's intent—the paper ballots the voters completed on Election Day.

Third, recounts are too difficult to obtain to serve as the requisite check. In Michigan, though the Board of State Canvassers initiated a recount based on Dr. Stein's petition, the state Court of Appeals stopped the count by reading into the state law a requirement that a candidate petitioning for a recount must establish that a recount could result in her winning the

[5] *See Berks County May Ask People To Vote Again in Two Precincts*, Associated Press, May 18, 2005, *available at* http://www.votersunite.org/article.asp?id=5408.

[6] The Verifier - Polling Place Equipment – 2016, https://www.verifiedvoting.org/verifier/#.

[7] Michigan only uses optical scan tabulation of paper ballots. Wisconsin uses a mix of paper ballots (tabulated through optical scan machines and hand counts) and DRE machines with voter-verified paper audit trails.

election. *Attorney Gen. v. Bd. Of State Canvassers*, No. 335947, 2016 WL 7108573 (Mich. Ct. App. Dec. 6, 2016), *appeal withdrawn*, No. 154862, 2016 WL 7189651 (Mich. Dec. 9, 2016), and *appeal denied sub nom. Trump v. Bd. of State Canvassers*, No. 154868, 2016 WL 7189653 (Mich. Dec. 9, 2016), and *appeal denied sub nom. Gen. v. Bd. of State Canvassers*, No. 154886, 2016 WL 7189664 (Mich. Dec. 9, 2016). This decision offers *no* standards for determining when a candidate is close enough to winning to request a recount, and will likely be cited to try to limit future recount petitions.

In Pennsylvania, candidates cannot initiate recounts. That task falls to voters. This year, voters who sought to confirm that their votes had been accurately recorded by requesting recounts were thwarted by a byzantine, unworkable legal regime. Three voters in each of the 9,158 election precincts in Pennsylvania must submit notarized affidavits to obtain a recount in that precinct. Whether a voter must request a recount in the county board of elections or in court depends on when his county finishes counting votes.[8] But county boards do not routinely disclose when they finish counting, and two of the state's largest counties (Allegheny and Delaware) admitted in court that their boards of elections do not comply with the legally mandated process for completing the count. Not even the state's top election officials knew when various counties had finished counting the vote; they provided inaccurate and contradictory information in response to inquiries from the Stein Campaign. As a result of erroneous guidance from the Pennsylvania Department of State and county boards' erratic compliance with shifting and secret deadlines, thousands of voters had valid recount petitions wrongfully rejected.

And the costs of recounts are prohibitive as well. Wisconsin estimated the cost at approximately $3.5 million (though the final amount may be higher or lower); Dr. Stein had to pay that amount before the recount began. In Pennsylvania, thousands of individual voters must pay a total of $457,900 in order to request a statewide recount (in addition to potential court filing fees of over $100 or even $200 per petition), and the Commonwealth Court demanded a $1 million bond from the voters who filed a contest proceeding. The financial burdens in Pennsylvania are so severe that they make anything close to a statewide recount practically impossible.

Fourth, none of the three states have any effective audit procedures. While Wisconsin and Michigan require a post-election audit, it does not require the audit to be completed before certification of the vote totals. And in Wisconsin, the audit is of a small sampling of the vote based on no discernible statistical methodology. As a result, our expert statistician testified that the audit cannot be expected to reliably detect errors or tampering. In Pennsylvania, the audit procedure is fundamentally inept because most voters vote on machines that have no paper trails and the audit does not include a forensic review of the voting machines.

[8] *See* 25 P.S. §§ 3154(e), 3261, 3262. The Pennsylvania Department of State interpreted these confusing deadlines at odds with the Pennsylvania Supreme Court. It told boards of elections to reject all recount petitions filed after the initial computation of votes, even though Pennsylvania's highest court has held that voters can file in the Board of Elections within five days after the initial computation is finished. *See In re Reading Sch. Bd. Election*, 634 A.2d 170, 172-73 (Pa. 1993).

**Moving Forward to Protect the Integrity and Accuracy of America's Votes**

The United States should investigate these irregularities and vulnerabilities. Why are 30% of Americans voting on machines that have no paper trail in light of the known vulnerabilities of any computerized voting system? Why is there insufficient funding to maintain voting machines in communities of color, resulting in widespread failure of machines on Election Day? Why are reliable, cost-effective audits not standard operating procedure? Why are voting machines connected to the internet notwithstanding the FBI Director's sworn testimony?

The nation's experts are unanimous in what needs to happen to ensure America's votes are counted accurately. *First*, all jurisdictions should use paper ballot-based systems. Every vote in this country should be backed up by a voter-marked paper ballot, available for a hand recount or an audit. *Second*, we need automatic audits, for every election, to verify the accuracy of the vote totals. Crucially, scientifically-based audits, termed "risk limiting audits," are far less expensive and more efficient than a full manual count, yet can provide reliable evidence so long as the audited "ballots are chosen at random by suitable means."[9] And where a recount is sought, there must be a right to a hand recount and (in the interim until we ensure a paper ballot for each vote) a forensic audit of all paperless machines. *Third*, we need to ensure adequate funding of our election system to maintain voting machines and train election staff. We need federal standards that ensure the integrity of our vote.

Our representative democracy is founded on voting for our elected representatives. It is both a paramount civic duty and a fundamental right. Americans need to be confident that our votes are counted accurately. We thank you in advance for your attention to this critical issue: Ensuring the integrity of our elections must be a nationwide priority.

Please let us know if you are in need of additional information or if we can assist this effort in any way. We look forward to maintaining a dialogue with the Department of Justice to the extent possible to follow up on this important issue.

Sincerely,

Jonathan Abady/LWV

Jonathan S. Abady

Encl.

---

[9] *See* Mark Lindeman and Philip B. Stark, *A Gentle Introduction to Risk-limiting Audits,* IEEE Security and Privacy, Special Issue on Electronic Voting, 2012, *available at*http://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

C. Vanita Gupta
Chris Herren
Mary McCord
Federal Election Assistance Commission

# EXHIBIT A

# OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

## HEARING

BEFORE THE

## COMMITTEE ON THE JUDICIARY HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 28, 2016

**Serial No. 114–91**

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

22–125 PDF WASHINGTON : 2016

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

Mr. ISSA. In light of the fact the Maryland Bar has this prohibition, would that have changed your view of allowing her in and saying you had no authority?

Mr. COMEY. I am not qualified nor am I going to answer questions about legal ethics in this forum. The FBI has no basis to exclude somebody from an interview who the subject of the interview says is on their legal team.

Mr. SMITH. Okay. Thank you, Director Comey.

Thank you, Mr. Chairman. I yield back.

Mr. GOODLATTE. The Chair thanks the gentleman, recognizes the gentlewoman from California, Ms. Lofgren, for 5 minutes.

Ms. LOFGREN. Thank you, Mr. Chairman.

And thank you, Director Comey, for once again appearing before this Committee, as you appear before so many Committees here in the House. Sometimes I wonder how you get any work done at all, that you are called up here so frequently.

You know, there has been a lot of focus on the private email that Secretary Clinton used, just as her predecessor, Colin Powell, used. So far as I am aware from the public comments, there is no forensic evidence that there was a breach of that server, although theoretically you could intrude and not leave evidence.

But there has been very little focus on the breach at the State Department email system. Now, it has been reported in the press that this breach of the State Department email system was one of the largest ever of a Federal system and was accomplished by, according to the press, either China or Russia.

I am wondering if you are able to give us any insight into whether it was, in fact, the Russians who hacked into the State Department email system or whether that is still under investigation.

Mr. COMEY. Not in this open forum, I can't.

Ms. LOFGREN. All right. I am hoping that we can get some insight in an appropriate classified setting on that.

Now, we have watched with some concern—and I know you are also concerned—about the Russian intrusion into our election system. It has been reported to us that the Russians hacked into the Democratic National Committee database. They also hacked into the Democratic Congressional Campaign Committee. And it seems that they are making an effort to influence the outcome of this election. We have been warned that the information stolen might not just be released but also be altered and forged and then released, in an effort to impact the election here in the United States.

Yesterday, there were press reports—and I don't know if they are accurate, and I am interested if you are able to tell us—that the Russians have also hacked the telephones of Democratic staffers and that there was a request for Democratic staffers to bring their cell phones into the FBI to have them mirrored.

Can you tell us anything about that?

Mr. COMEY. I can't at this point. What I can say in response to the first part of your question, any hacking is something we take very seriously. Any hacking in connection with this Nation's election system is something we take extraordinarily seriously, the whole of government. So it is something the FBI is spending a lot of time on right now to try and understand. So what are they up to and what does it involve and what is the scope of it to equip the

President to decide upon the appropriate response. And so that is one of reasons I have to be very careful about what I say about it. That work is ongoing. I should make clear to folks when we talk about our election system, there has been a lot of press reporting about attempts to intrude into voter registration databases. Those are connected to the Internet. That is very different than the electoral mechanism in this country, which is not.

Ms. LOFGREN. We had actually a hearing, and I had the chance to talk to Alex Padilla, who is the Secretary of State in California. Number one, they encrypt their database. And number two, even if you were to steal it, there is backups that you couldn't steal. So they can't really manipulate that. But you could cause a lot of damage. I mean, you could create chaos on Election Day that would—and you could target that chaos to areas where voters had a tendency to vote for one candidate over another in an attempt to influence the outcome. So it is not a benign situation certainly, and one that we want to worry about.

I want to just quickly touch on a concern I have also on cyber on rule 41, and how the FBI is interpreting that. I am concerned that the change, as understood by the FBI, would allow for one warrant for multiple computers, but would include allowing the FBI to access victims' computers in order to clean them up. Cybersecurity experts that I have been in touch with have raised very strong concerns about that provision, especially using malware's own signaling system to disable the malware. The cyber experts who have talked to me and expressed concern believe that that ultimately could actually trigger attacks. And, so, I am wondering if you have any comments on how the FBI intends to use rule 41 *vis* malware on victims' computers?

Mr. COMEY. Yeah. Thank you.

Mr. GOODLATTE. Time of gentlewoman has expired. The witness will be permitted to answer the question.

Mr. COMEY. Thank you, Mr. Chairman. I am not an expert, but one of the challenges we face, especially in dealing with these huge criminal botnets, which have harvested and connected lots of innocent peoples' computers is how do we execute a search warrant to try and figure out where the bad guys are, and get them away from those innocent people? And the challenge we have been facing is to go to every single jurisdiction and get a warrant would take, literally, years. And so we are trying to figure out can we use rule 41 to have one judge issue that order and give us that authority.

Ms. LOFGREN. Mr. Chairman, I know my time has expired. I would just like to close by expressing the hope that the FBI might seek the guidance of some of the computer experts at our national labs on this very question of triggering malware attacks. And I yield back.

Mr. GOODLATTE. The point is well taken. The Chair recognizes the gentleman from Ohio, Mr. Chabot, for 5 minutes.

Mr. CHABOT. Thank you, Mr. Chairman. Director Comey, Chairman Goodlatte, in his introduction of you, mentioned that you are a graduate of the College of William and Mary. And as you may well know, I am a graduate of William and Mary as well.

Anyway, you may remember that our alma mater is very proud of something called the honor code. And I checked out the wording

communicated to me. And the FBI reached its conclusion as to what to do uncoordinated from the Department of Justice.

Mr. KING. Even though Justice was in the room with your investigators? And I would make that final comment and I yield back. Thank you, Chairman.

Mr. COMEY. Sure. Sure.

Mr. GOODLATTE. The Chair thanks the gentleman. The Chair recognizes the gentleman from Georgia, Mr. Johnson, for 5 minutes.

Mr. JOHNSON. Thank you, Mr. Chairman. Russian hacking into the databases of the Democratic National Committee and the Democratic Congressional Campaign Committee, as well as Russian hacks into the voter registration systems of Illinois and Arizona, serve as ominous warnings to the American people about the risks that our electoral processes face in this modern era. Unfortunately, Trump Republicans in the House are as obsessed with Hillary Clinton's damn emails as Trump has been about President Obama's birth certificate. Just like The Donald closed his birth certificate investigation after 5 years of fruitless investigation, however, I predict that the Trump Republicans will, at some point, close this email persecution. The American people are sick of it. The attention of the American public is increasingly focused on the security of this Nation's election infrastructure. On Monday, the Ranking Members of the House and Senate Intelligence Committees, Senator Dianne Feinstein and Congressman Adam Schiff, issued a joint statement setting forth the current status of this investigation. It said this: "Based on briefings we have received, we have concluded that the Russian intelligence agencies are making a serious and concerted effort to influence the U.S. Election." They work closely with intelligence community individuals to be able to put that statement out to the American public.

Director Comey, I don't want to ask you about any classified information, but is their statement accurate?

Mr. COMEY. I don't—I can't comment on that in this forum. As I said in my opening, we are investigating to try to understand exactly what mischief the Russians might be up to in connection with our political institutions and the election system more broadly. But I don't want to comment on that at this point.

Mr. JOHNSON. Free and fair elections are the linchpin of our society. A compromise or disruption of our election process is something that this Congress certainly should be looking into. Would you agree with that?

Mr. COMEY. I can't speak, sir, to what Congress should be looking into. But the FBI is looking into this very, very hard for the reasons you say. We take this extraordinarily seriously.

Mr. JOHNSON. Thank you. In June, the FBI cyber division issued a flash alert to State officials warning that hackers were attempting to penetrate their election systems. The title of the flash alert was, "Targeting Activity Against State Board of Election Systems." The alert disclosed that the FBI is currently investigating cyber attacks against at least two States. Later in June the FBI warned officials in Arizona about Russian assaults on their election system, and hackers also attacked the election system in Illinois, where they were able to download the data of at least 200,000, or up to 200,000 voters. In August, the Department of Homeland Security

convened a conference call warning State election officials and offering to provide Federal cyber security experts to help scan for vulnerabilities. And yesterday it was announced that at least 18 states have already requested election cybersecurity help to defend their election systems.

Director Comey, since these flash alerts and warnings went out over this summer, I would appreciate you letting us know whether or not there have been any additional attacks on State operations or databases since June.

Mr. COMEY. There have been a variety of scanning activities, which is a preamble for potential intrusion activities, as well as some attempted intrusions at voter registration databases beyond those we knew about in July and August. We are urging the States just to make sure that their dead bolts are thrown and their locks are on, and to get the best information they can from DHS just to make sure their systems are secure. And again, these are the voter registration systems. This is very different than the vote system in the United States, which is very, very hard for someone to hack into, because it is so clunky and dispersed. It is Mary and Fred putting a machine under the basketball hoop at the gym. Those things are not connected to the Internet. But the voter registration systems are. So we urge the States to make sure you have the most current information and your systems are tight. Because there is no doubt that some bad actors have been poking around.

Mr. JOHNSON. All right. With that, I will yield back the balance of my time. And thank you, sir.

Mr. GOODLATTE. The Chair recognizes the gentleman from Texas, Mr. Gohmert, for 5 minutes.

Mr. GOHMERT. Thank you, Mr. Chairman. And Director Comey, thanks for being here. I was a bit astounded when you said the FBI is unable to control who a witness, coming in voluntarily, brings in to an interview. I have seen a lot of FBI agents tell people who could come into an interview and who could not. And in this case, and I am sure you have heard some of the questions raised by smart lawyers around the country about providing immunity to people like Cheryl Mills in return for her presenting a laptop that you had every authority to get a subpoena, and if you had brought a request for a search warrant, based on what we now know, I would have had no problem signing that warrant so you could go get it anywhere you want. And in fact, I have talked to former U.S. attorneys, A.U.S.A.s, who have said if an FBI agent came in and recommended that we gave immunity to a witness to get her laptop that we could get with a subpoena or warrant, then I would ask the FBI not to ever allow this agent on a case.

Can you explain succinctly why you chose to give immunity without a proffer of what was on the laptop, give immunity to Cheryl Mills while she was an important witness, and you could have gotten her laptop with a warrant or subpoena?

Mr. COMEY. Sure. I will give it my best shot. Immunity we are talking about here, and the details really matter, that we are talking about, is act of production immunity, which says we want you to give us a thing. We won't use anything we find on that thing directly against you. All right? It is a fairly——

# EXHIBIT B

STATE OF WISCONSIN CIRCUIT COURT DANE COUNTY

BRANCH 3

* * * * * * * * * * * * * * * * * * * * *

| | |
|---|---|
| In the Matter of the Recount of Votes for President of the United States:<br><br>JILL STEIN,<br>c/o Emery Celli Brinckerhoff & Abady LLP<br>600 Fifth Avenue, 10th Floor<br>New York, NY 10020,<br><br>Petitioner,<br><br>vs.<br><br>WISCONSIN ELECTIONS COMMISSION,<br>212 East Washington Avenue<br>Third Floor<br>Madison, WI 53707, and<br><br>Members of the Wisconsin Elections Commission, each and only in his or her official capacity:<br><br>MARK L. THOMSEN, ANN S. JACOBS, BEVERLY GILL, JULIE M. GLANCEY, STEVE KING, and DON M. MILLIS<br>212 East Washington Avenue<br>Third Floor<br>Madison, WI 53707,<br><br>Respondents. | Case No. 16CV3060 |

* * * * * * * * * * * * * * * * * * * * *

PROCEEDINGS: HEARING

DATE: November 29, 2016

BEFORE: The Honorable VALERIE BAILEY-RIHN,
Circuit Court Judge, Branch 3, Presiding

APPEARANCES: Attorney CHRISTOPHER M. MEULER,
Freibert Finerty & St. John,
Two Plaza East, Suite 1250,
330 East Kilbourn Avenue,
Milwaukee, Wisconsin 53202,
appearing on behalf of the Petitioner.

APPEARANCES: (Con't)

Attorneys MATTHEW D. BRINCKERHOFF,
DEBBIE GREENBERGER and DAVID A. LEBOWITZ,
Emery Celli Brinckerhoff & Abady LLP,
600 Fifth Avenue, 10th Floor,
New York, New York 10020,
appearing as counsel on behalf of the
Petitioner.

Assistant Attorneys General S. MICHAEL MURPHY,
COLIN ROTH, DAVID V. MEANY, ANDREW COOK, and
ANTHONY RUSSAMANNO,
Wisconsin Department of Justice,
17 West Main Street,
PO Box 7857,
Madison, Wisconsin 53707,
appearing on behalf of the Respondents.

MICHAEL HAAS,
Wisconsin Election Commission,
Madison, Wisconsin, appearing in proper
person.

Attorneys JOSHUA L. KAUL and
CHARLES G. CURTIS, JR.,
Perkins Coie,
One East Main Street, Suite 201,
Madison, Wisconsin 53703,
appearing on behalf of the Intervenor
Secretary Hillary Clinton.

REPORTER: Melanie Olsen
Official Reporter

* * *

MR. KAUL: No questions, your Honor.

THE COURT: All right. We'll hang up on you now. Thank you very much for your time.

THE WITNESS: Thank you very much.

(End of call.)

THE COURT: Any further witnesses?

MR. BRINCKERHOFF: No further witnesses. Although, we would, if possible, subject to the Court's permission, like an opportunity to make an oral presentation at the end of the evidentiary piece.

THE COURT: Certainly. Any witness for the defendant?

MR. MURPHY: Our first and only witness will be Mike Haas.

THE COURT: Okay.

MICHAEL HAAS,

called as a witness, being first duly sworn, testified on oath as follows:

THE CLERK: The chair does not move; the microphone does.

DIRECT EXAMINATION

By Mr. Murphy:

Q. Good afternoon, Mr. Haas. Could you state your name and spell it for our court reporter.

A. Sure. Michael Haas. M-I-C-H-A-E-L, H-A-A-S.

Q. Thank you. And what is your job?

A. I'm the administrator of the Wisconsin Elections Commission, which is the state agency that administers and enforces election laws in Wisconsin.

Q. I'm going to have you elaborate a little bit on that. What are your job functions? What do you do day to day? What do you oversee?

A. I oversee our staff of approximately 30 positions. A few of our chief responsibilities are to train and provide guidance to local clerks, county clerks and municipal clerks, who conduct elections. We publish or issue guidance in a variety of forms. We conduct training, webinars, and in-person training. We attempt to administer and implement and interpret any new legislation dealing with elections. Our staff also reviews nomination papers or election petitions that are filed at the State level. We maintain -- develop and maintain the statewide voter registration system, which is a database containing all the States' registered voters. We certify election results, among

other tasks.

Q. I'm going to ask, could you expand on that a little bit. So during and after an election, what are your tasks?

A. The agencies'?

Q. No. Well, the agency to the extent you oversee it, but regarding your knowledge.

A. Well, our tasks are, as I said, to work with clerks, work with candidates, work with the legislature, state officials, other agencies, work with federal and state agencies on securing election systems. Our agency also tests voting equipment, approves voting equipment for use in the state of Wisconsin.

Q. Okay. Let's talk a little bit about the voter equipment. What types of equipment does the state of Wisconsin use for voting?

A. Wisconsin, being one of the most or the most decentralized election system -- administration system in the country, we have 1854 municipalities. They are responsible for purchasing the voting equipment used in their municipality often purchased in coordination with the county clerk. And there's a variety -- a handful of different types of voting equipment used in the state. But generally speaking, it's optical scan tabulating equipment and electronic equipment --

A. Correct.
Q. And they can't do a forensic audit, correct?
A. Correct.
Q. And they can't do a review of the source code, correct?
A. Correct.
Q. You also testified that most often the equipment is programed by a private vendor for each election specifically, correct?
A. Right.
Q. And that private vendor creates the ballot software in their own offices, correct?
A. I would assume so.
Q. Okay. And they create that software on computers, correct?
A. Again, I would assume so.
Q. And you have no way of knowing sitting here today whether those computers are connected to the Internet, correct?
A. Not directly, correct.
Q. And it's fair to say that it's likely that those computers are connected to the Internet, right?
A. I don't know.
Q. You've never required that your private vendors keep their computers not connected to the Internet,

correct?

A. The State does not. You're correct.

Q. And who the private vendors are that contract with the municipalities in Wisconsin is public information, correct?

A. Yes.

Q. Okay. And that's information that somebody who was interested in a cyber attack could determine, correct?

A. If they go to our website, sure.

Q. It would be as simple as going to your website?

A. Correct.

Q. Okay. So, just so I understand this, the ballot software is placed onto a form of removable media; is that accurate?

A. Yes.

Q. Okay. And that removable media is at some point inserted into the voting machine before the election, right?

A. Right.

Q. But the software gets onto the removable media by being connected to an actual computer, right?

A. Yes.

Q. And that actual computer is located in a private vendor's office, correct?

A. Again, I'm assuming it is. I don't know specifically where they program the media.
Q. Okay. And you already said that you have no way of knowing one way or the other whether that computer in the private vendor's office is connected to the Internet?
A. Yes. Correct.
Q. You also testified that you -- that the State of Wisconsin conducts post election audits; is that correct?
A. Yes.
Q. Okay. And those post-election audits are explicitly not to verify that the vote count was accurate, right?
A. It is to confirm that the voting equipment tabulates the votes as it should. It is not intended to be a recount or determine the winner of an election.
Q. And it's not used to verify the results of the election before they're certified, right?
A. Correct. The clerks can conduct the audit before or after the certification of the results.
Q. And the audit, you said that there's a number of counties that are chosen but -- and that there's various adjustments, correct?
A. Number of municipalities, not counties.