STANDARDS BOARD OF ELECTION ASSISTANCE COMMISSION

IN RE: (COMPUTERS AND ELECTIONS: THE GROWING POTENTIAL FOR CYBER VOTE FRAUD)

SPEAKER: STEVEN STIGALL

_____)

DATE: February 27, 2009
PLACE: Double Tree Hotel
5780 Major Boulevard
Orlando, Florida 32819

JULIANA M. CARY, FPR
Court Reporter
Notary Public, State of Florida at Large

KING REPORTING & VIDEO CONFERENCE CENTER, INC.
14 Suntree Place, Suite 101
Melbourne Viera, Florida 32940

(Brief introduction omitted per the request of Mr. Stigall and Attorney Tamar Nedzar.)

MR. STIGALL: As I said, there's an interesting reason why I'm here today. I'm not here to produce any smoking gun that shows you that electronic voting is insecure or anything like that. For several years, I've worked with others in my organization to try and identify foreign threats, emphasis on foreign threats, to important U.S. computer systems.

A few years ago it occurred to us that that should include potential foreign threats to the computers upon which our elections in this country are increasingly dependant. Now, obviously the first question in your mind is, okay, did my organization actually discover any foreign threats to the computers upon which our elections are increasingly dependant.

I'm going to say this: We're in an open, unclassified forum. Rest assured that if we ever were to discover specific and credible information

about foreign threats to our critical U.S. election computers, we would do in my organization what we've done since 1947. We would bring that attention to the most senior policy makers in the

country, and they would act accordingly.

What I'm here to do today, today, is to share with you the results of some research that we undertook some years ago and which we continue to do. I can advance here.

Basically, when I look at a computer, when I look at an election system, I'm not an election analyst. I'm not a political analyst. We have folks like that where I am, and they know how to parse foreign elections that we've followed. I do not look at an election system the way a political candidate would look at it. I do not look at an election system the way a party chairman might look at it, the way the media looks at it.

When I look at an election system, I see a computer system, because increasingly that's what they are. And to the extent that there are foreign actors who have shown an interest in developing unauthorized access to U.S. computer systems, that's where I get interested in it.

What I did was I looked at foreign elections

in countries that are often for the first time trying to have relatively free and fair democratic elections. This involves not only the computerization of their elections, but, as I said,

it's often the first real election they've ever had.

All of you come from different states, different parts of the country. We're all working together to try to come up with guidelines and standards, things like that.

The countries that I looked at, they had to go from typically communist dictatorship to relatively western-style democracy. And in some cases, overnight in terms of their election system. So all the challenges and issues that we are, that you are dealing with that have surfaced, they tend to surface in some of these countries right away, early on, and in a big way. And basically it's those issues that have surfaced that is what I'm going to be talking about today.

I have exactly two slides that address so-called Internet voting. I understand the issues behind that here in this country. I'm not here to address issues surrounding it in this country, but rather to share with you some of the experiences

that foreign countries have had when they've attempted this, and some of the challenges that remained for them in that regard.

Again, a couple of important points that lay

out where we're going here. Where I come from, we do not do vulnerability assessments of any U.S. systems. We do not look at U.S. systems. What we do is we identify foreign threats to those systems, and we relay that information via a variety of mechanisms to the owners and operators of those systems.

Typically the owners and operators, typically but not always, are going to be the U.S. Government. And that's basically what we do. That's the line of work I'm in.

And secondly, I'm not going to go down here and address specific types of voting machines, or specific companies that are making voting machines, or anything like that. I'm not going to do that. We're talking about the foreign experiences that other countries have had as they attempt to computerize their elections, as they attempt to bring their electoral process into the 21st century.

As I said earlier, I am not a politician,

political analyst. I don't look at this perhaps the way folks in your line of work do. I look at, looked at this as a computer network, as a computer security issue. And I did not really know how to

begin this research effort, so I went to the people that do look at elections overseas, and I got some ideas on how to proceed.

And basically I came up with a model. It's an arbitrary model, but it worked, I think. And basically I divide an election process in terms of the computer's role in that process into five separate steps. These don't all occur on election day. Keep that in mind.

Basically what I'm saying, you heard the old adage, follow the money. Here I follow the vote. And wherever the vote becomes an electron and touches a computer, that's an opportunity for a malicious actor potentially to get into the system and tamper with the vote count or make bad things happen.

The rest of my presentation will address these basic five steps. The first one, of course, occurring long before election day, and the fifth one on election day, and afterwards. But that's how we're going to proceed, one through five.

First thing I discovered -- and a lot of this may be old news to you. But again, I'm not a political analyst, so this was an eye opener to me. Is that what we saw happening is the first thing,

if you're a foreign country, again, coming out of the Soviet era, for example, or some other form of autocracy, you need to update your voter registration list. Maybe you don't even have a voter registration list. And typically these countries are doing this on computer.

This often takes the form of folks spanning out across the country with lap tops or whatever and writing down names. Sometimes it occurs in the foreign version of the county courthouse, or indeed, the national capital itself, in which the registrar, or whatever they call the person, they're presented with a box of documents. And they said, here is our tax is rules, or here is our census rules, or here's the old voter list, put it on the computer.

And the registrar has a challenge right away. Because if you encounter an error on the old list, an obvious error, someone who is deceased or whatever, do you faithfully transcribe that error onto the computer system where you immediately

introduce error to the new computerized database, or do you deliberately weed out that person's name, because you know he's dead, and try to make the new computerized list as accurate as possible.

Well, it's a damned if you do, damned if you don't situation we saw overseas in that either way you're going to have errors pop up. I have some examples of that coming up. As you all know better than I, it's who gets the vote is often as important as anything else.

One thing I was continuously reminded of in looking at this, if you look at that very bottom bullet there, I'm not so much looking at shenanigans on election day as I am all of the things that foreign actors try to do to try to effect the outcome of the election long before election day. And the next slide here, there are some examples, some specific examples that we saw of this.

I think and this is -- by the way, this is the country of Georgia, not the state. I cannot emphasize that strongly enough. I'm only here to talk about foreign examples. I think we're all familiar with the phenomenon of someone who has been dead for a couple years still appearing on the

voter lists.

In Georgia, they raised this to a whole new art form in which they went back to the 18th century to try to bend the rules. Really creative

stuff there.

The second bullet says Albania. It's actually about Macedonia. I actually discovered something three days ago. The U.S. Government has different names for that country that some people call Macedonia. And I don't want to offend the Macedonians in the audience. It's a sensitive issue, what do we call Macedonia, but this was in the country some people call Macedonia.

They computerized their voter registration lists. And it turns out there's a sizable ethnic Albanian presence in that country, in Macedonia. And the folks back in Albania noticed that there weren't a lot of Albanian identifying names on the new Macedonian voter lists.

And we've seen pretty colorful uses of the word genocide over the years, and I thought this one probably takes the cake. Voter genocide the Albanians were accusing the Macedonians of doing.

More seriously and one thing you should be aware of, this example came out of Latin America in

which a hacker did actually try to get to the computer that held the voter names, the database where the voter registration was. This illustrates a very important point. And that is any computer

hooked up to the Internet either through a wire or through a wireless connection is a porthole for hackers. You heard that. I'm here to confirm it very simply.

Now, this example on the bottom bullet there, according to the authorities, the hacker did not actually get into that database, but he achieved access to the computer where it was located. It was just arguably a matter of time until he had figured out how to get past the various security procedures that were in place.

This again raises the issue you may -- if you think the computer is not hooked up to the Internet, there's a variety of things that also are in play. We now have, of course, wireless connections. Perhaps a wireless connection is enabled, spy share is enabled, this kind of thing. It's no longer enough since (inaudible) with a 6K modem wire.

A computer that's hooked up to the public Internet is problematic in this regard. And

computerized registration of voters is the first indication we see that there's a potential for fraudulent behavior in the electoral process.

Here is a little quote from the Taliban in

Afghanistan. Some of us think it's a courageous thing to vote on election day for some of these countries. It's as equally courageous to show up and register to vote. If you've got the list of the people registered to vote, you have a list of targets, if you're a bad actor.

Give you a second to read that.

All right. I'm going to move ahead now to the election day photograph. (Inaudible) that is a photograph of a Venezuelan voting machine. These machines are not -- again, I'm not here to parse particular voting machine examples of some of the things we look at. Some of the companies overseas, emphasis on overseas, that manufacture these machines carry on their web site information about how they have a SIM card reader, Ethernet jack, USB ports. In other words, there's ways of networking these machines.

An electronic voting machine is a computer. That's the way we look at it. It has memory, (inaudible), it has software built into the

hardware of the machine to tell it what to do.

Most interestingly, not only can it be networked, but it can be interrogated outside. It's a computer. That's essentially where it is.

And because it's a computer, it carries with it all the vulnerabilities that the computer has.

Now, I'd like to talk a little bit about Venezuela later on. We're not here to pick on Venezuela, per se. It's an interesting example of some of the things we think can happen.

I don't really like the phrase e-voting, because I think it (inaudible). It doesn't really tell me what I need to know. If you're talking about an electronic voting machine, that I understand. If you're talking about Internet voting, that's something else.

Again, when we look at the foreign countries that we looked at, you see two models. Either the machines themselves are networked to each other at the polling station and are then connected to another computer at the polling station, and that computer is not what you cast ballots on. It's just connecting all the information from those machines. Then the voting information is sent from that computer downstream or upstream, as the case

may be.

Or you have a situation in which the machines again appear to be stand-alones, but again, on election day, folks are removing the flash card

memory that records the votes. Again, these are scenarios that you will not be alien to, but what we're looking at is foreign experiences of security threats with these type of things.

The first question one asks about these voting machines is are they password protected. Well, there's passwords and then there's passwords. Is the password the name of your granddaughter? Is it the name of your pet? If it is, I'm going to have that password in an hour. Not me personally, but I mean, a dedicated hacker. That's what they do.

If it's a so-called strong password in which you use a mix of letters, numbers, and special characters, you do greatly complicate the task for a malicious hacker. But then you have to ask yourself, are the passwords changed from election to election, or is it the same.

And our favorite scenario where I come from is your password P-A-S-S-W-O-R-D. You would be surprised. Again, who has access to that password is really terribly important.

And the bottom tick on this slide is really crucial. That's why I buried it at the bottom of the slide. That is the actual physical security of these machines long before election day is crucial.

When I look at a foreign country and I suspect that the regime may be playing games with the computer component of the election system, one of the first questions I ask is where are those machines stored, or were they stored, period, long before election day and afterwards. And I want to know if those machines can be interrogated electronically, remotely on election day. Is there a wire or connection connecting those machines to, quite frankly, the public hearing them?

I understand the wireless issue is one thing that has been addressed. I'll be talking a little bit more about that particular question. Okay.

Again, this slide, I want to talk about that. Again, I think you all probably know a little bit more about this than I do. Bottom line is all the countries I've looked at, yeah, about 36, 37 countries, all the scenarios by which they use electronic voting, they produce a paper ballot receipt, and it's part of the social contract that they have.

Now, at this point, I would make my only hand-waving generalization of the presentation, which is always risky. In the countries that I looked at, you're dealing with voters who have

never seen a computer before, let alone used one. When they've had elections in the past, some of these societies do not accept voter fraud, but they understand it's going to happen. And the idea of a local party boss throwing a shoe box or ballots in the river, that's part of the background noise. They understand that a little bit of fraud at the local level will occur.

When you introduce computers into the process, I found in some of these northern cultures you are introducing a level of opacity. You are removing a bit of transparency that makes them uncomfortable. And that's something that I think is worth keeping in mind.

We tend to view computers as things that modernize, that allow certain efficiencies that would otherwise be impossible. Again, I'm looking at foreign cultures. This is a phenomenon that emerged.

The machine puts out a paper receipt. The person sees the paper receipt. So even though they

may have never seen a computer before, they can look at that paper and say, hey, this is how I'm going to do this. The person puts the receipt in the box.

In all the countries I've looked at, you have to ask several questions. First of all, if there is a discrepancy at the end of the day between the machine count and the paper count, which has legal priority? Some countries spell that out very clearly. Other countries, like Russia, it's kind of hey, maybe it's deliberately so. I don't know.

Also, they have to determine what will trigger an automatic recount, what will be the required difference between the two counts before you have to have a recount. In some countries -- in one country, for example, the difference is only one percent. In another country, the difference is .001 percent. I can't do the math standing up here. (Inaudible). So different countries are going to have different standards for the difference they're going to allow between the paper count and the electronic count.

Now, again, what I said, traditionally in a traditional voting scheme, the greatest opportunity for fraud that we've seen in other countries is at

the local level. When you introduce computers into the equation, you're moving that fraud upstream, and you're allowing a single point, electronic single-point failure. Meaning the potential for

mischief can occur higher up the food chain electronically, much faster, and affect a lot more people in terms of the vote count than would be the case if fraud occurred at an individual level, where, again, you're talking about the classic scenario where ballot boxes get thrown in the river or fraudulent ballots get produced. Here it's electronic.

One of the cases that we looked at in terms of the potential for messing with the computers at the precincts, at the local level is what kind of voting machines are you using. For example, in Russia, they cannibalize whatever computer they can find in many cases. Often this involves classroom computers that kids are using one day in the classroom, and the next day it's blessed as a voting machine. They go in, they put software in it.

Of course, then you have to ask yourself how good was the security check on the computers that you're using before this. It may not be an issue

in this country, but it's a huge issue overseas.

What computers are you using? Are you cannibalizing just regular desktop computers to be voting machines? Are you bringing in dedicated

voting machines?

In Russian, again, 94,000 precincts. I refer to Russia often in this briefing simply because it's a country that I've studied closely, and they provide us with a lot of interesting examples of this phenomenon.

We did see an interesting situation develop in Venezuela in 2000. This is a matter of public record. At that time, there were 19,000 voting machines. I showed you a picture of them earlier in that country.

It's important to understand that Hugo Chavez controlled, himself, his people, every facet of the computer side of that election. I don't like reading from the slides. I would not do so up here. The bottom line is it was all covered. He had, all parts of the chain of custody were under his control or his people.

Now, what happened was there was a referendum Venezuela in August 2004 about whether or not to recall Hugo Chavez. It was basically a yes, no

kind of -- they had the vote. Chavez won, and that recall petition was defeated. And what happened afterwards is kind of interesting.

Usually when I give this presentation, I've

got two different colored markers, and I can go to the board and illustrate this. I have do it verbally here.

Basically, some Venezuelan mathematicians crunched the numbers, and they looked at the difference, the differences between the vote that Chavez got when he originally ran for president I think in 2000 and the votes that he got in the recall referendum in 2004. They discovered that the delta between those two counts in certain areas where they believe Chavez's support was weak was consistent across the board.

In other words, in those areas where Chavez knew he was going to need some votes, the difference between the number of votes he got in 2000 and 2004 was the same from region to region. And the mathematicians produced lots of interesting facts, and figures, and statistics to show that this was statistically really not possible.

And they used that as an argument for Chavez, because of his complete control of the voting

machines, the voting machines and their infrastructure, that Chavez was able to insert computer code into the system to adjust the vote surreptitiously.

Now, understand, this is nothing as blunt as a vote against Chavez registers as two votes for him. It's not that blunt. It's much more subtle. It registers as 1.1 votes for him. I'm making this up to illustrate the point.

It was a very subtle algorithm these people think they found, but there was a problem. You immediately see what the problem was in red on the bottom of the slide. You have 19,000 voting machines each spitting out a paper receipt. People walk that receipt over to the box, put it in the box. And it's the paper receipts that are going to be counted at the end of the day.

They push the button on the voting machines. The voting machines say this is how many votes are cast on me. You count the number of ballots, and there's a difference in the outcome. So we had to ask ourselves, how do you defeat the paper trail. How do you defeat the paper ballots the machines spit out? Those numbers must agree, must they not, with the electronic voting machine count. How do

you defeat the paper route?

It turns out in order to figure that one out, you have to stop thinking like a political analyst, you have to stop thinking like an academic, or a

person from the intermedia, or whatever, who follows the election as an unfolding story, and you have to start thinking like a Third World autocrat. You can defeat the paper vote with the guys with the guns. They put the votes in the boxes and take the votes out to the trucks, take them to the military barracks. (Inaudible).

Again, you have the paper vote count, you have the electronic vote count. You have to figure out how to reconcile those two if you are going to commit fraud. In this case, he simply took a gamble..

Now, I'm going to back up one. If you look at that second bullet, okay, we're going to audit some of the electronic voting machines, and we're going to audit them at random. Chavez agreed to allow 100 of the 19,000 voting machines to be audited. If a huge pattern or a significant pattern of discrepancies arises, he has a problem then.

It is my understanding -- this is in red. It is my understanding that the computer software

program that generated the random number list of voting machines that were being randomly audited, that program was provided by Chavez. That's my understanding. It generated a list of computers

that could be audited, and they audited those computers. You know, no pattern of fraud there.

But again, if you are bent on large scale fraud at the national level, and you know you have a fraudulent paper count and trail, you have to do something with that paper count.

A huge issue for us as we look at this issue is how do you get the votes from outlying precincts back typically to the capital of the country. Again, as you all know better than I, in foreign countries, you typically have one central national level election commission as opposed to you tell me.

This is a huge issue if you're a country in southeast Asia that, you know, your country consists of 80,000 islands. (Inaudible). It's nice to have results come in so the people know who won the election the next day rather than wait for three weeks for all the ferries and such to come in from different islands with the vote count, or people phone them in.

You saw a lot of problems with these countries when you transmit them electronically realtime on election night. I understand this is an issue you're looking at. I'm not going to address that

here.

But what the foreign experience has been is that these vote counts are typically going to be transmitted in much the same way as you would send an e-mail attachment. That is, it's going to be an e-mail attachment. It's going to write out over the public Internet using Internet protocols, using protocols that a lot of people understand. Good actors and bad actors.

And that's why the basic -- I'm trying to avoid the Latin, sine qua non. The basic, most important thing here that we ask is, that we look at is whether or not these votes are being encrypted. Now, I want to say a word about encryption.

It's a scary word. (Inaudible). People see the word encryption and they dive for cover. I'm not going to go into a tutorial on how encryption works.

Bottom line is if you encrypt the electronic transmission of votes from point A to point B, you

greatly complicate the tasks of the what would be attacker who would get into the data stream and adjust the numbers. Greatly complicate their task. You do not remove the threat of a so-called

denial-of-service attack.

There's two kinds of denial-of-service attacks. The first is where a bunch of computer guys jump all over your computer and clobber it, overwhelm it with Internet traffic, and shuts it down, or you have to shut it down. That's a classic computer attack. If that occurs on election night, it does not effect the actual count of the votes, but nobody looks good if they have to go in front of the cameras and explain how hackers were able to launch a denial-of-service attack and you can't get votes from the outlying regions of the country.

The second kind of service attack is (inaudible). I'm not going to go there. The point is if the votes are encrypted from point A to point B, you greatly complicate a hacker's job.

But there's more to it than that, because you then have to ask yourself is the data encrypted before it's transmitted or is it encrypted after it's been received. In other words, so-called

encryption of, quote, data at rest, unquote.. This is another important issue to look at.

Again, encryption, I wouldn't say it solves a lot of the problems, but it creates a lot of

problems for those who want a system and have a lot of problems.

If your country consists of 11 or 12 time zones, realtime on election night is very attractive. Especially when everything has to flow back to Moscow. We already mentioned 94,000 precincts. That's a lot. I do not know how many we have in this country.

They solved the problem in Russia in terms of how to deal with hackers, whoever, serious actors, getting into the vote stream on election night. It looks like in Russia the votes are transmitted -- I don't like reading from the slides here. But the same computer system, the same band they use for classified government communications is what they use to send the votes over on election night. Which is to say the same government authority in Russia that is responsible for electronic spying, electronic eavesdropping, what people in my role call SEGAT, those are the people running the vote transmittal on election night. I'm here to tell

you, without making recommendations, that's a pretty secure system.

I'm not going to sit around waiting for the U.S. Internet to designate a percentage of the CIA

and National Security Agency to be responsible for cyber transmittal in the U.S. e-mail. Not expecting that to happen, nor am I recommending it. But in Russia they solved that problem by doing that.

The ballots obviously are encrypted. Again, they're going over otherwise classified communications. And I think the bottom line there speaks for itself. Russian hackers are busy making money doing other things besides messing with elections.

The word on the street is they may look the other way if you hack a foreign target, but if you go against a Russian bank or a Russian government computer system, you may end up as a speed bump somewhere. So don't do that. Pretty secure system.

We're going to talk more about Russia in a minute. All right. Again, when you look at all the reports from overseas about where the computer vote fraud is most likely to occur, if you judge it

simply by where all the reports and in the various foreign press and whatever discuss, it's pretty clear that the central election headquarters, which is where all the computers are processing the

votes, or for one computer, this is a place where a lot of this can occur.

We talked about the idea of an algorithm, some sort of computer program that adjusts votes as they're coming in. I have an example of that coming up. Again, the big challenge for someone who would use cyber means, computer means to tamper with an election is not only dealing with the paper vote count, but how much of a vote can you manipulate maliciously before you trigger an audit. That becomes important in the Ukraine, as you will see in a moment.

We discussed already the defeat or not defeat of a paper receipt. We've heard of the so-called colored revolutions in recent years. In the Ukraine, they call it the Orange Revolution. See all the orange banners folk are waving there?

The gentleman there, Mr. Yushchenko, elected to run his country in 2004, but he wasn't elected to run his country in October of 2004. And here is why: The way this story is typically portrayed is

there's a situation in which they had the election in October. The crowd didn't like the result. The crowd smelled fraud. They couldn't prove it. They piled into the streets, and then you had the Orange

Revolution. It was a little more interesting from there.

What happened was they did have the voting in October. There was allegations of fraud on the part of Mr. Yushchenko's PM, Mr. Yanukovych. He was an old-guard type of official who Moscow believed would bring the Ukraine back into the Russian fold. And as we say in Washington, remember it's not the scandal, it's the cover-up that will kill you.

Because in Ukraine what happened on election night is they had a plan in place whereby they introduced an unauthorized computer into the Ukraine election committee national headquarters. They snuck it in. They had a couple people on their side working on it. I don't know exactly how this worked, but the implication is that these people were monitoring the vote count coming in from different parts of the country, and they were making subtle adjustments to the vote. In other words, intercepting the votes before it goes to the

official computer for tabulation.

Now, at that point, something very interesting happened. The head of Mr. Yanukovych's campaign the director of his campaign, the campaign director

started making a series of cell phone calls to these guys on the inside. And he's asking them, did you erase the wrong files, did you cover up access, did you clean yourself up. In other words, he's not really asking them did you pull off the scam the way we agreed, because it's already been pulled off. He's asking them if they did the cover-up okay.

Very shortly, in short order, in short order, Ukrainian newspapers published the transcripts of these cell phone conversations. That's kind of interesting. At that point, the crowds fled into the streets. Public outrage reaches critical mass. There's an agreement to hold a second election in December, and Mr. Yushchenko is elected. (Inaudible).

Finally, on election night -- understand that in the countries that we look at they don't have cable news services to report realtime election results county by county, state by state. In many of these countries, the Internet is increasingly

the go-to source for late-breaking information, late-breaking information on election night.

And typically what you see happen is the national election commission or central election

commission, whatever they call it, they are doing realtime vote totals on the Internet on their web site. Again, this is an example you would see in Russia. Just pull those down and use it for this purpose..

Now, it's very important to understand this is a web site where when someone attacks a web site we tend not to get terribly excited. It's sort of equivalent to taking a can of electronic spray paint and defacing something. But we do ask ourselves some questions.

Number one, you want to make sure in these countries that we looked at that the computer that is posting the web site, number one, is not the computer that's also processing the votes, and number two, is not connected in any way, shape, or form to the computer that's collecting the votes.

We've only seen one example overseas in which it looks like the election authorities actually use the same computer to count the votes for the country that they use for their web site. And

hackers did get into it in I believe 2004, 2005. Kind of embarrassing.

Does not -- other than that though, assuming all they do is deface the web site, typically all

they're going to do is embarrass people. They're not actually going to touch the official vote count. But to the extent that these emerging democracies in other countries are trying to do a free and fair election in the right way, you don't want obviously that to happen on election night.

I do want to segue now very briefly into the question of Internet voting. I know this is an issue of great importance to you all. I'm not here to, again, parse or critique specific proposals. Simply understand I come from an organization that watches what foreign hackers do and other organizations. We've seen some foreign experiences with this, and they haven't figured out how to do it yet.

There's one example to look at in a moment. Switzerland, which might be working for them, I leave it to you discern the degree it would work in this country.

Bottom line, we're talking again about any computer hooked to the Internet. Obviously I'm not

talking about a situation solely where military personnel overseas would go to one place and cast a ballot on one machine from their homes and offices. The UK has tried this. Finland and some of the

Baltic Republics have done some experiments with this. We'll talk about a Russian example coming up.

Again, eventually where this is leading overseas, emphasize where this is leading overseas is voting with any mobile wireless device eventually.

Now, there are some real issues that these countries have to grapple with. I defer to you the extent of which these are applicable to us. Authentication of voter ID obviously is a huge issue. The Swiss, see how they deal with that, how they determine who is the person at the keyboard, either that they're at home, the office, Internet cafe, shopping mall, whatever. How do you determine that really is the person that they claim to be, and they're legally allowed to vote.

The second one though is a huge issue overseas. That's absence of duress. We're talking about a situation in which a woman will have acid thrown in her face if she doesn't vote the way her

husband tells her to vote.

Also absence of duress, we have a situation in one country we looked at in which everyone in a factory was led down onto the shop floor, and they

had an absentee ballot station set up, electronic. And everyone in the factory said, here is how you're going to vote. I assume you don't have a problem with that if you want to continue working here.

And that's, again, another example of a faceless electronic vote scheme. There's an absentee before election day so the party officials and factory officials could make sure everyone voted the same way.

Privacy of vote is a little bit different than absence of duress. I don't have to tell what percentage of computers are out there that have unauthorized voting software on it. Do they have key stroke auditors? Do they have other forms of software that records what you do on your computer that's violating or compromising your privacy?

When you buy a computer, take it home, I am told that as soon as you plug it in, firewalls not withstanding, anti-virus software not withstanding, if you just plug that computer in, within minutes

someone or something is pinging on that system to see how vulnerable it is.

You've heard of the phrase botnet, B-O-T-N-E-T. Botnets, which are out there in vast

numbers, Botnets are simply large clusters of computers that have been relatively poorly defended, and hackers have gone into them to place codes on them so those computers can help the hacker do something on the day he chooses. Again, privacy of vote. There is software, malicious software on the computer being used which would compromise the voter's privacy.

I don't have to tell you that probably 95 percent of us in this room are all using the same operating system. We know what it is.. Hackers know that, too.

Now, I refer a lot to hackers in this presentation, but understand, I'm not really concerned about the 18-year-old wannabe. I'm concerned about the 28 or 38-year-old folks who have been doing this a long time and may be under contract with someone from an organization. In other words, to thwart an election or compromise a computer in that context.

This brings us to a great example, Russia. A

few weeks ago, the head of the Russian Central Election Commission, Vladimir Churov, made an interesting proposal. He met with representatives of the Russian hacker community.

I do not know the extent to which this was a representative cross-section of Russian hackers. It was sponsored by a Russian magazine, hacker magazine, which is interesting.

Vladimir Churov held the event. He said in early March we're going to test a new voting system in Russia. We're going to test it for five years. I want you people to come in, give us your best shot. We're not interested in people who really want to harm maliciously the system, but if you want to test our system to try and identify new vulnerabilities. We're going to reward you if you do this. We're not going to say what the reward is.

But this is an example of an alternative to, you know, bringing in what I call old people. You know old people. People in their 40s and 50s. When you know what you are doing the day some of your colleagues were born, you qualify as an old person, which is why I feel old sometimes.

But what Mr. Churov is proposing is something

different from a controlled red team experiment where you bring in old people to test your system. He's talking about turning this over to hackers in the wild. A situation in which you can be

guaranteed that vulnerabilities will be discovered that you had no idea were there, or just as important, see how many approaches are there that perhaps you had discounted as you were developing. Well, we thought about that, but we decided that wasn't a viable alternative or a viable way of compromising the system. Well, some hotshot 24-year-old over there may think otherwise, and Mr. Churov is going to find out. So that's one of the issues we look at.

I do want to deal briefly with the Swiss example. It's an interesting example. Still use it as a case study for a pilot project for Internet voting.

They issued scratch cards to voters, for lack of a better phrase. The election authority did. You received the scratch card. You scratch off the thing to reveal a pin. You go to the their web site on election day, and you enter that pin into the web site, and then they ask you a question. And I think one of the questions was what canton

was your mother born in. Canton means roughly equivalent to state.

It was a calculated risk that in a small country that if a hacker or some nefarious actor

gets your card, or gets a whole bunch of cards, they've got a pin number, but they're not going to know where your mother was born or some other piece of uniquely biographical information that you have to associate with that particular card. It's a risk that they would not be able to associate that biographical data with the pin number in such numbers to throw the election. Again, it's a calculated -- it's risk management rather than risk avoidance. Again, place of birth, this type of thing. The Swiss endeavor.

The UK tried Internet voting. One of the reasons to do it was to enhance voter turnout. The there was a small -- they made voter kiosks out in public was the model that they used. So as you're walking home from work, on your way to town, or whatever, you can stop at the kiosk and vote. They did see an increase in voting there, but in their own words, it was statistically inconsistent.

I'm just going to conclude by summarizing on this. Again, when I look at foreign election

systems, I'm not -- don't get me wrong. I'm not probing it for what kind of vulnerabilities it has to attacks. I'm simply looking at the computer to see what type of vulnerabilities other people might

be trying to use to destroy it, because that may be applicable in this country.

Again, when we look at election systems overseas, to the extent that they even have computers, I look at them as a computer network. And computer networks have all the vulnerabilities that any computer network has, whether it's an election system or whatever.

The physical security of the machines has emerged as a big issue long before election day, who has access to them, and who programs these machines, and who has access to that programming. Again, just old-fashioned physical security on election day.

We talked about the sociological factor of decreasing the transparency for some cultures that introduce computers. I'm not going to propose it's entirely relevant here, but I add it for what it's worth.

You saw a lot of problems. I say you don't solve a problem. You create problems for an

attacker by turning those votes into meaningless scrambles, ones and zeroes, on the data screen out there.

And we concluded with a note about so-called

Internet voting, where the foreign experience has been in the form of pilot projects, again, in the UK, Baltic Republics. Russia has very serious -- Russia wants to move the situation I believe by 2010 where people can vote with cell phones. They're very serious about that. As Russia moves to a one-party state, they're trying to make their elections available to everyone so everyone can vote for the one party. So that's the irony.

I will conclude on that note. I thank you for your attention. Again, I'm not here to tell you there's (inaudible), explain why electronic voting is, but to show some foreign experiences that I've had in introducing computers into their election systems, and the extent those experience overseas may be revealing to the kind of work we're trying to do here. That's why I'm here. I believe I will -- shall I take questions or --

MS. BARTHOLOMEW: You have time.

MR. STIGALL: Few minutes for questions. Sure. I will always forget to repeat the

question. I guess we have a mike here. Everyone can hear the question.

MS. DEBEAUVOIR: Dana DeBeauvoir, Austin, Texas. Could you please go back to the Chavez

election. I'm just a little dense. I didn't quite get it as to when Chavez took possession of the vote part. I conceive it's the boxes and some of them had sleeves of the boxes. What was point I can seeing, you know, the capture of all that information. What did they do to it to make it different? I mean, it's there (inaudible).

MR. STIGALL: The argument that the opposition in Venezuela made was that Chavez had introduced a surreptitious code into the voting system to adjust the vote. The problem is if you get a discrepancy between what you see the machine says and what the paper ballots say, you have to explain that discrepancy, unless you take physical custody of the paper ballots and say there was no discrepancy.

Then you move the paper ballots to the barracks, military barracks, and then you assume no one is going to raise a big enough stink where you have to open up the barracks and review the paper ballots. That was the charge the opposition made.

MS. CHAPMAN: Beth Chapman, Alabama.

Couple questions. Based on your presentation today, would you be willing to say that Spain has the better model than the other countries that you studied?

MR. STIGALL: Ma'am, I really can't speak to Spain. I'm sorry. I can't speak to them specifically.

MS.. CHAPMAN: I'm sorry. Switzerland. I'm sorry. Spain. Any of those S words.

MR. STIGALL: I was listening on the radio yesterday. The person on the radio said it Sweden, not Switzerland. I used to live in Switzerland. It's one of those places where people die falling off their farms. It's a vertical country.

You may think of Switzerland as being a very homogenous country. The reality is they have four major languages, fourth a very small minority.. They do have four officially recognized languages, which has many different groups within them. They also have a large immigrant population. So it is an increasingly diverse demographic group. A tremendous sense of -- again, my second hand-waving generalization, sociologic generalization. It is a country with a tremendous sense of civic duty.

When I lived there, every Saturday morning

teenagers throw their rifles over their shoulders and ride out to the range to prepare for militia training.

MS. CHAPMAN: What's wrong with that?

MR. STIGALL: Nothing. I'm just saying they have a very community view of themselves. And to the extent of issuing cards to each voter, scratch the card, match that data with each biographical identifying data to you, to the extent that would be applicable here, that's for you all to determine.

The Swiss example is probably the most well thought out example we've seen. Although, the exact mechanics of the system that they've tried in Baltic countries, in the UK, I'm not familiar with the exact mechanics of that.

MS. CHAPMAN: I guess what I'm interested in as Secretary of the State is really studying this issue which I have vendors coming to me saying they're doing this in other countries. Those countries are Spain, Australia, and UK. You did mention the UK. I'm very interested in what you are learning about those other countries that was not presented today.

I guess playing devil's advocate, what

concerns me here when I hear your presentation is that ballots can be taken away from a group, which we saw that happen in some of our states I'm embarrassed to say. That voters can be put under

duress, which in my state they are many times. That they're told to vote a certain way or they'll lose their benefits or security of their jobs. That people can manipulate the equipment. Worse case scenario, people could. They don't, but they could.

We're not saying let's vote on anything. We're saying secure military Internet voting. Because the military, as I understand it, did create the Internet, so that makes it a little more credible. And we don't have a dictatorship like Chavez, where one person is in charge of everything. And we do have a checks and balances.

And so I'm asking you to tell me, or anyone to tell me why we should be any more concerned about Internet voting, because there are less numbers of people that can hack the Internet in the levels to which we're concerned about than are physically hacking absentee ballots in my state.

MR. STIGALL: The simple question is (inaudible). It's a question of risk management

versus risk avoidance. That's the short and simple.

Yes, sir.

MR. WARE: I'm Steve Ware from California.

I'm not exactly sure the total number of voting places in the United States, but I've always operated off of about 200,000. I'm not exactly sure there's others that we know about. But I did attend a conference that we talked about an Internet voting model in Australia for their military overseas voters. And the advocates of that seemed to think there was a good Australian model to that. Not blanket Internet voting, but more of a secure system.

Are you familiar with that at all?

MR. STIGALL: No, sir, I'm not. Again, in the military installation, you're going to have control. That increases the comfort factor. Yes. That's a fair assessment.

MR. HARRIS: Allen Harris from Arlington, Virginia.

In your example of Switzerland, the question that occurred to me is how do they acquire these backup information, where do they keep it, and how vulnerable is the backup information.

MR. STIGALL: That hits a very important point. We hear a lot about attacks with threats to financial systems. It is probably fair to say the financial data is probably the best backed up data

out there, financial data.

In the Swiss example, I don't know the extent to which it's backed up, but that is one of the fundamental boxes you need to check in terms of overall network security. Backing up the data, and backing it up on a computer different than the one you're trying to backup.

MR. HARRIS: The Swiss example, have they garnered something from their banking system?

MR. STIGALL: I cannot say.

MR. HARRIS: They're very secure with those I know.

MR. STIGALL: That's an interesting two dots to connect, and I cannot connect them.

MR. HARRIS: The other question, if I may, had to do with the paper receipts that were dropped in the box. And apparently, if I understand it correctly, are they counted at the precinct level?

MR. STIGALL: Yes. That's a very important point.

MR. HARRIS: And how difficult would that be

if you have an election that had many offices being filled, and constitutional amendments, and bond issues, and things of that kind, how does that --

MR. STIGALL: Admittedly, I think it's

probably fair to say, sir, that the elections I'm looking at overseas, you're voting for parties.

MR. HARRIS: That would be fair.

MR. STIGALL: Now, the flip side of that is in some countries there's dozens of parties. So the ballots can be cluttered in that regard, but they tend to be kind straight up or down situations. So they are counting them at the local level, making sure the electronic count matches the paper count, then proceeding accordingly.

MR. HARRIS: Now, I think at least in my county, the security that you mentioned about emitting, transmitting from the precinct to the central place, we do that by telephone. We call them in. Now we can't with the electronic machines. We still use -- can't get any more of them. Still use what we got. We don't do that, because a neighboring jurisdiction tried to do that, much bigger, and they just had a malfunction of the telephone lines. There wasn't any hacking or anything. But we have them phoned in.. But they

are unofficial, and they don't become official until we really look at them. And occasionally people misread. I think we have a backup system at least as to the reporting. That's why I wondered

if some of these --

MR. STIGALL: They use a variety of systems besides electronic transmittal to get those from the outlying precincts to the capital city. Sometimes it's a situation where they take the flash card out of the computer voting machine, they collect the flash card memories in a box and transport those to the central election authority.

But where it gets interesting is when you look at countries that do transmit electronically, because they have such a vast geography that's how they have to do it. But telephones are used also to do it overseas. I'm primarily only concerned when I see the digitized votes touching a computer.

MR. HARRIS: Thank you.

MR. LINDBACK: John Lindback from Oregon.

I think you're get a lot of questions about Switzerland because of your assessment that that's probably the one that's most secure that you've seen.

MR. STIGALL: I'd say that it's the one most

thought out.

MR. LINDBACK: I was concerned about their other registration system. (Inaudible). Obviously in each voter's record is the name of their

mother's birth place. That kind of information is not historically part of voter registration records in America.

Are they working off a civil registry that has that information already?

MR. STIGALL: The short answer is I don't know. Again, what the Swiss are doing is they have made the assessment that you're not going to see enough of these cards compromised in such a way to throw an election, that a malicious hacker would know that biographical data to associate it in an automated way. That is an important point to get across.

Worry about computer fraud here, not other forms of fraud. If you're talking about a particular village or section where they've got a few dozen or few hundred of these cards, and they're taking the time to go back and figure out, okay, this guy, I know where he was born, whatever, I'm not really looking at the old, typical kind of fraud. I'm only concerned about when electrons

become maliciously tampered with.

MS. DEBEAUVOIR: Just to follow up -- Dana DeBeauvoir, Austin, Texas.

Just to follow up on John's question then, so

there is a step in the process whereby the pin number and the mother's birthplace, both of it stacks up against something that says, yes, that's correct.

MR. STIGALL: That's a very important point on the web site of the election authority. They have to reconcile those two numbers. Your question of whether or not that information was preexisting on the registration lists, that's a valid point and, again, raises the issue where is the voter registration before the election.

Is it sitting on a computer that's hooked up on the Internet? Is it sitting on a computer connected to another computer that's hooked up to the Internet?

Basically that gives me an opportunity simply to reassert that this, the security of these elections, that use of computers begins long before election day, and that the computers that hold that voter registration data should be nailed down in terms of their security, just as you would secure

an electronic voting machine on election day. That's what that earlier slide on voter registration was trying to convey.

You don't want it hooked up to the public

Internet in terms of voter registration data if you're concerned about securing those things. There are countries overseas that put your information on the Internet because they want to say, look how many people we've registered to vote.. But putting it on the Internet is different from keeping the official record off the Internet away from hackers.

I thank you for your attention. Again, perhaps some of this is insight to you.