DISTRICT COURT, DENVER COUNTY, COLORADO 1437 Bannock Street Denver, CO 80202	DATE FILED: September 17, 2021 8:12 PM FILING ID: E9E5DD591D201 CASE NUMBER: 2020CV34319
ERIC COOMER, Ph.D., Plaintiff vs. DONALD J. TRUMP FOR PRESIDENT, INC., et al., Defendants	▲ COURT USE ONLY ▲
Attorneys for Plaintiff Charles J. Cain, No. 51020 ccain@cstrial.com Steve Skarnulis, No. 21PHV6401 skarnulis@cstrial.com Bradley A. Kloewer, No. 50565 bkloewer@cstrial.com Zachary H. Bowman, No. 21PHV6676 zbowman@cstrial.com **CAIN & SKARNULIS PLLC** P. O. Box 1064 Salida, Colorado 81201 719-530-3011/512-477-5011 (Fax) Thomas M. Rogers III, No. 28809 trey@rklawpc.com Mark Grueskin, No. 14621 mark@rklawpc.com Andrew E. Ho, No. 40381 andrew@rklawpc.com RechtKornfeld PC 1600 Stout Street, Suite 1400 Denver, Colorado 80202 303-573-1900/303-446-9400 (Fax)	Case Number: 2020cv034319 Division Courtroom: 409
EXHIBIT H-1	

DISTRICT COURT, CITY AND COUNTY OF DENVER
STATE OF COLORADO
1437 Bannock Street
Denver, CO 80202

^ COURT USE ONLY ^

ERIC COOMER, Ph.D.,
Plaintiff,

Case Number 20CV34319

Courtroom 409

vs.

DONALD J. TRUMP FOR PRESIDENT, INC., SIDNEY POWELL, SIDNEY POWELL, P.C., RUDOLPH GIULIANI, JOSEPH OLTMANN, FEC UNITED, SHUFFLING MADNESS MEDIA, INC., dba CONSERVATIVE DAILY, JAMES HOFT, TGP COMMUNICATIONS LLC, dba THE GATEWAY PUNDIT, MICHELLE MALKIN, ERIC METAXAS, CHANEL RION, HERRING NETWORKS, INC. dba ONE AMERICA NEWS NETWORK, and NEWSMAX MEDIA, INC.,
Defendants.

VIDEO-RECORDED REMOTE DEPOSITION OF CHANEL RION

August 9, 2021

REMOTE APPEARANCES:

FOR THE PLAINTIFF:

CHARLES A. CAIN, ESQ.
BRAD KLOEWER, ESQ.
Cain & Skarnulis PLLC
P.O. Box 1064
Salida, Colorado 81201
Telephone: 719-530-3011
Email: ccain@cstrial.com
bkloewer@cstrial.com

REMOTE APPEARANCES (Continued):
FOR DEFENDANT DONALD J. TRUMP FOR PRESIDENT, INC.:
JOHN ZAKHEM, ESQ.
Jackson Kelly, PLLC
1099 Eighteenth Street, Suite 2150
Denver, Colorado 80202
Telephone: 303-390-0016
Email: jszakhem@jacksonkelly.com
FOR DEFENDANTS CHANEL RION and HERRING NETWORKS, INC., dba ONE AMERICA NEWS NETWORK:
BERNARD J. RHODES, ESQ.
BRAD JOHNSON, ESQ.
Lathrop GRM LLP
1515 Wynkoop Street, Suite 600
Denver, Colorado 80202
Telephone: 720-931-3200
Email: bernie.rhodes@lathropgpm.com
THOMAS M. ROGERS III (TREY), ESQ.
Recht Kornfeld, PC
1600 Stout Street, Suite 100
Denver, Colorado 80202
Telephone: 303-573-1900
Email: trey@rklawpc.com

FOR DEFENDANT SIDNEY POWELL & SIDNEY POWELL, P.C.:
BARRY ARRINGTON, ESQ.
Arrington Law Firm
3801 East Florida Avenue, Suite 830
Denver, Colorado 80210
Telephone: 303-205-7870
Email: barry@arringtonpc.com

FOR DEFENDANT JAMES HOFT:
JONATHAN C. BURNS, ESQ.
P.O. Box 191250
St. Louis, Missouri 63119
Telephone: 314-329-5040
Email: tblf@pm.me

REMOTE APPEARANCES (Continued):
FOR DEFENDANT ERIC METAXAS:
MARGARET BOEHMER, ESQ.
THOMAS B. QUINN, ESQ.
Gordon Rees Scully Mansukhani, LLP
555 Seventeenth Street, Suite 3400
Denver, Colorado 80202
Telephone: 303-534-5160
Email: mboehmer@grsm.com
tquinn@grsm.com
ERIC P. EARLY, ESQ.
Early Sullivan Wright Gizer & McRae, LLP
6420 Wilshire Boulevard, Seventeenth Floor
Los Angeles, California 90048
Telephone: 323-301-4670
Email: eearly@earlysullivan.com

FOR DEFENDANTS JOSEPH OLTMANN, FEC UNITED, and SHUFFLING MADNESS MEDIA, INC. dba CONSERVATIVE DAILY:
ANDREA M. HALL, ESQ.
The Hall Law Office, LLC
P.O. Box 2251
Loveland, Colorado 80539
Telephone: 970-419-8234
Email: andrea@thehalllawoffice.com
FOR DEFENDANT MICHELLE MALKIN:
GORDON A. QUEENAN, ESQ.
Patterson Ripplinger, P.C.
5613 DTC Parkway, Suite 400
Greenwood Village, Colorado 80111
Telephone: 303-741-4539
Email: gqueenan@prpclegal.com
FOR DEFENDANT DEFENDING THE REPUBLIC:
MICHAEL W. REAGOR, ESQ.
Dymond • Reagor, PLLC
8400 East Prentice Avenue, Suite 1040
Greenwood Village, Colorado 80111
Telephone: 303-734-3400
Email: mreagor@drc-law.com

REMOTE APPEARANCES (Continued):
Also Present (via videoconference):
Peter Scott
Charles Herring
Bobby Herring
Abbie Frye
Peter Scott
J. Gray

PURSUANT TO WRITTEN NOTICE and the appropriate rules of civil procedure, the video-recorded remote deposition of Chanel Rion, called for examination by Plaintiff, was taken via videoconference, commencing at 12:01 a.m. EST, on August 9, 2021, before Sara A. Stueve, Registered Professional Reporter and Notary Public in and for the State of Colorado.

I N D E X

P R O C E E D I N G S

* * * * *

THE VIDEOGRAPHER: Here begins the deposition of Chanel Rion. Today's date is August 9, 2021. The time is 12:01.

Counsel, please identify yourselves and state whom you represent.

MR. CAIN: Well, what we're doing in lieu of that is making appearances via email for those that are not directly involved.

But for the record I will certainly state my name is Charles Cain, and I represent the plaintiff.

MR. RHODES: And I'm Bernie Rhodes, and I represent OAN and Chanel Rion and will be defending the deposition on behalf of Ms. Rion today.

THE VIDEOGRAPHER: Will the court reporter please swear in the witness?

THE REPORTER: Yes, after I read in the statement regarding the remote proceedings:

The attorneys participating in this deposition acknowledge that I am not physically present in a deposition room and that I will be reporting this deposition remotely. They further acknowledge that, in lieu of an oath administered in person, the witness will verbally declare his/her testimony in this matter is given

under penalty of perjury.

The parties and their counsel consent to this arrangement and waive any objections to this manner of reporting.

If there are any objections, please state them at this time.

Hearing none, Ms. Rion, will you please raise your right hand?

CHANEL RION,

having been first duly sworn to state the whole truth, testified as follows:

DIRECT EXAMINATION

BY MR. CAIN:

Q. Can you state your full name, please?

A. Yes, Chanel Rion.

MR. REAGOR: Do we have the continuing stipulation that an objection by one party will stand as an objection for each defendant?

MR. CAIN: Yeah. And so we don't have to continue to -- to acknowledge that, I would say that I certainly would stipulate, until anybody else objects to that arrangement, that that's an ongoing stipulation for all of the deposition.

MR. ARRINGTON: And I agree with that.

THE REPORTER: I'm sorry. Can I get the name of

the attorney who made that statement?

MR. REAGOR: Michael Reagor.

Q. (By Mr. Cain) Okay. How are you doing this morning, Ms. Rion?

A. I'm good, as good as a parent of a newborn can be at this moment.

Q. Congratulations to you on that. We'll try to get through this as quickly as possible.

Have you done a Zoom deposition before?

A. I have not.

Q. Have you done any kind of deposition before?

A. No, I have not.

Q. All right. I assume you've had a chance to meet with your counsel in preparation for giving testimony?

A. I have.

Q. All right. Did you -- did you spend some time reviewing documents in order to also prepare for your testimony?

A. Yes.

Q. Give me a thumbnail of what you did to prepare.

A. I just collected documents that I think your -- you had requested of us and sent them over, and I explained the context of those documents.

Q. And about how much time did you spend collecting documents and reviewing them in order to testify today?

A. I don't recall.
Q. More than an hour?
A. Yes. I was pulling down documents that -- I had to dig through old emails and things like that. So yes, more than an hour.
Q. Well, in terms of ground rules you -- you sat in on at least one other deposition; right? I think Mr. Herring's?
A. Yes.
Q. Okay. It's a little -- still trying to do this by video -- we'll do our best. I will show you some documents and share my screen, hopefully, from time to time.
But it's important that we get your testimony here today and not the testimony of others. And by that, I mean you are not to communicate with others electronically. I can't see your screen or your phone.
So during the course of giving testimony, will you agree that you won't be communicating with other parties?
A. Yes, of course. The only other party I might be communicating with is my newborn, who might interject occasionally. But we'll try and keep that at a minimum.
Q. Well, hopefully, you won't have to consult -- is it a -- is it a girl? Did you have a girl?

A. I had a boy. It will be baby's first deposition. We'll get to put that in the baby book.
Q. Is your newborn in the room with you?
A. He is, yes. He's next to me.
Q. I'll try to use my soothing voice.
A. Appreciate it.
Q. Other than not communicating with other parties, the other couple of ground rules that I like to ensure is that you understand my questions. I tend to ask sometimes long-winded questions. Sometimes I ask halting questions, and you will interject.
But the important thing is that you and I are on the same page. So if I ask you something and you don't get what I'm asking, you don't understand what I'm asking, will you stop me and ask me to phrase my question so that you understand?
A. Yes.
Q. All right. Great.
And we won't be here long, but if you need a break, that's perfectly fine. We probably will take one or two. The only caveat there is you have to complete your answer to a question that I have on the table before you take a break. In other words, no timeouts during the pendency of a question. Okay?
A. Understood.

Q. All right. Since you sat in on Mr. Herring's testimony, you should have heard him say that you conducted extensive research in connection with the "Dominion-izing the Vote" report.
Can you explain to me what specific research and investigation you did in connection with that specific report that was aired on OAN?
A. Of course. I had been working on this OAN Investigates special for several weeks. I was looking into documents that were submitted by Congress to voting measuring companies, the three that dominate the market now.
I was looking at congressional hearings. These were all publically available documents.
Was watching prior media reporting on election vulnerabilities. There were quite a few to pull from, especially between 2016 and 2020.
I had seen -- I had been reading the reports that were being put out by hackathons, like Voter Village's DEF CON meetings. They would put out reports and findings for the vulnerabilities they were identifying in election systems in the United States today.
I had been reading documents from secretary of state's offices. They would put out reports about the

security of their elections.
I had consulted -- I had seen several documentaries on this, including Kill Chain -- HBO's Kill Chain, where they laid out, you know, the hackathon that I just mentioned by DEF CON. They would talk about the vulnerabilities in our system today.
These were some of the things that I looked at in -- in researching, generally, for the "Dominion-izing the Vote."
And then, of course, I had interviews included in the actual final product.
Q. Is it fair to say -- you said several weeks. Can you be any more specific than that?
A. I can try to be. I think it was mid-October when I first started reading and, kind of, mulling over the topic and thinking about ways to put this into a cohesive piece to air on OAN.
Q. Was the idea behind the germination of this piece your own, or were you consulting with others at OAN about running that type of the report?
A. I don't recall whose idea it was. I mean, this was a -- as a news organization, we're dealing with the news of the day, and the news of the day at the time was very much the question of whether or not our elections were secure.

So this was something that we discussed -- we, as a network, discussed amongst each other. I don't know whose idea it was, but I was certainly working on it once I started working on it.

Q. And you were physically located, as you are now, in Washington, D.C. during this time period?

A. Yes, sir.

Q. And you produced this piece out of Washington, D.C.?

A. Yes, sir.

Q. Who in Washington was assisting you on this piece?

A. In Washington, I had a videographer/editor. I don't recall all the videographers that may have worked with me at the time, because we shoot in pieces. But we had -- Young Richardson was my editor for this piece.

Q. Can you spell that name, please -- the first name please?

A. Young, Y-o-u-n-g.

Q. And that you call your videographer and editor. So this would be the person who would have done the camera work while you were doing your piece and then would edit the video?

A. Yes. And, again, I preface that with he may not have been the only videographer to be taping for me at the

studio. Because I don't remember the exact -- how -- how -- how long I actually taped in the studio. But we would have various videographers work with us at any given time.

So he may not have been the only videographer physically taping my stand-ups, but he was certainly the editor.

Q. Okay. And like, I guess, I alluded to, this all occurred -- the studio you referred to would have been in D.C. as well?

A. Correct.

And if you'll notice on my -- in "Dominion-izing the Vote," behind me is the White House when I'm doing the stand-ups. So I was at the White House when I was taping portions of this piece.

Q. Okay. Have you covered, at least in general, the research and investigation that you did prior to recording this piece?

A. Didn't we just -- did we just go over that? Or is this a question --

Q. Yeah. I just was giving you an opportunity to -- if there's anything else that you neglected to mention, to -- to summarize that for me.

A. Well, of course, we listened to Michelle Malkin's interview of Joe Oltmann when it came to

be the -- the Eric Coomer portion of our piece.

I discussed this with a handful of hackers that I was able to discuss details with offline. LinkedIn -- I mean, there were a variety of routes that I had used to do my research. But I think gave you a good overview of what I did.

Q. Okay. Well, we'll talk about some of the offline discussions in a minute.

I want to -- I guess what I'm trying to cover is more the physical research in terms of documentation. You said -- and I won't repeat it -- but you went through hearings and reports and things of that nature.

I will tell you that I got, late yesterday, a letter from Mr. Rhodes that had a report attached to it. I think --

A. That may have been DEF CON 27's report.

Q. Okay. And that's one of the --

(Simultaneous speakers.)

A. -- a couple years' worth of reports. I specifically looked at DEF CON 27. I think that was August 2019, if I'm not mistaken.

Q. Okay. Well, we'll take a look here in just a second.

Actually, while I'm asking you some questions --

MR. CAIN: Rebecca, can you mark as the next

exhibit, 56? In my private folder, I think it's 10-A. It's OAN 1627 through 1680.

MS. DOMINGUEZ: Yes, sir.

Q. (By Mr. Cain) And while she's doing that, Ms. Rion, you had indicated you had the one videographer that help you work on this piece in Washington. Was there anybody else, in terms of OAN staff in Washington, that worked with you on this report?

A. I believe -- if I'm at the White House and I'm taping at the White House, Jay Thompson may have been the videographer.

But again, I think there were several videographers involved. I don't remember which ones were all involved in the physical taping of the piece.

Q. And while Mr. Richardson or another videographer may have edited the video was there anyone that edited your script that you wrote for the piece?

A. No, sir.

Q. So this was really, literally, your baby?

A. Well, I would discuss this with Charles Herring over the phone. I would talk to him about what I was finding and what I was putting together.

So he may not have physically been, you know, writing my script, but we were talking about what I was working on. So to the extent -- I hope that answers your

question.
Q. How involved would you characterize Mr. Herring in this "Dominion-izing the Vote" piece?
A. I would say fairly -- he was involved in, kind of, the overview of it, not so much the individual details of the report. So I didn't receive editorial guidance, but we discussed what I was working on.
Q. And other than -- since you said Mr. Herring didn't provide editorial guidance, was there anybody at OAN who did?
A. Not that I recall.
Q. And going back to your earlier testimony when you talked about the research you did, you said it took several weeks, may have started in the mid-October time frame.
Is it fair to say at the time that you began thinking about this piece and working on it, it was not intended to be a piece about Dr. Coomer?
A. No.
Q. Or, for that matter, Mr. Oltmann?
A. Not at all, right.
We had -- I had been lining up interviews for this particular piece long before I was even aware of Dr. Coomer's existence or Joe Oltmann's existence.
So they -- they ended up landing on my radar

around the time that Michelle Malkin did her interview on November 13th or so.
So about a day after or so, we started looking into Joe Oltmann's story and his accounting. And then we started looking into Eric Coomer. And that's about -- that's about -- about a week or ten days or so before the piece went to air.
Q. Well, was it -- did that affect your air date? In other words, were you planning on doing this investigative report on the 21st when it aired?
A. I did not have a date set. I -- it's -- it's -- usually when we're working on these investigative pieces, they are submitted when they're finished. And I did not have a set date for this piece.
Q. Gotcha.
A. We were not in any particular rush to put it out. I mean, it was just one of those stories that we thought was evergreen.
It was talking about election-system vulnerabilities, and that did not -- it wasn't like we were rushing toward an election date or anything like that. It was -- it would be finished when it was finished.
Q. I gotcha.
Ms. Rion, I'm going to share my screen so that

we can quickly look at Exhibit 56.
(Plaintiff's Exhibit Number 56 was introduced.)
Q. (By Mr. Cain) Do you see that okay?
A. Yes. DEF CON 27 Voting Machine Hacking Village.
Q. And this is one of the reports you referred to previously; correct?
A. Correct.
Q. And you'll just see I've marked it as Exhibit 56.
And in terms of this particular piece, it looks like it was coauthored by Georgetown University Professor Matt Blaze. Do you see that?
A. Yes.
Q. And do you consider Professor Blaze to be authoritative on the subject of election vulnerability?
A. I don't -- I cannot speak to Matt Blaze's entire career or his -- his credibility. But I can attest to the fact that the findings in this report were credible to me as I read it.
Q. Okay. And what findings, as you sit here today, in particular did you rely on in order to compile your report?
A. There were several things. I don't know if I can list all of them off the top of my head.
But one of the major findings of this report was

that Dominion Voting Systems had a way where hackers were able to access the machines, access the USB ports, access various portals of the Dominion machine. And they were able to hack into it and install video games, for instance.
They were able to do so, I believe, in the words of one of the hackers, undetected. So this was highly relevant to me as I was reading the report.
Q. So you read this report and the others. Did you actually look at -- and we don't have time to go through this, but you'll just confirm this is the report that you're referring to with the findings that you stated; correct?
A. Yes, sir.
Q. All right.
And as you said, you can't speak for the credibility of Professor Blaze, but you did find his -- his -- the work done and the findings credible in that particular --
A. If I'm not mistaken, there are over half a dozen names on that -- on that list of coauthors. So I don't -- again, I can't -- I don't know Matt Blaze. I have never met him. I don't know of his full resume.
But their findings seemed to speak for themselves. And there's quite a few coauthors in that

report.
Q. Well, if you found the findings were credible, I assume you felt comfortable in relying on Professor Blaze's work in this respect and his coauthors'; correct?
A. Correct. But I don't know what part of the report he actually coauthored.
So again, I don't want to misspeak and say that I know Matt Blaze or his resume. But the report in its entirety seemed reasonable to me when I was reading it.
Q. As part of your investigation leading up to producing this report, did you speak to Professor Halderman?
A. I did not. But I used -- I used some of his work. I've read some of his testimony before Congress, I believe, in 2018. I also -- I used a clip of Professor Halderman in my piece.
Q. Let's make sure we are talking about the same gentleman.
A. I believe Mr. Halderman was the individual who was able to -- I think he participated in the DEF CON events, hackathons, and he was -- he was a voice that New York Times, Axios, Congress -- they all relied on his expertise when it came to the hackability of the voting machines and our votes system in the United States.

MR. CAIN: Rebecca, can you mark as the next exhibit, Exhibit 10-B in my private folder.
Q. (By Mr. Cain) I believe this is going to be a screenshot, Ms. Rion, of Professor Halderman. I want to make sure, again, we're talking about the same gentleman.
Can I ask you what your son's name is while we're waiting for the exhibit?
A. Sure. We named him Atlas.
Q. Any expectations there?
A. Yes. Actually, right behind me is a letter from President Biden congratulating his birth. I don't know if you can see it. Can you see it?
Q. I can't. I can see what you're talking about, though.
A. He wished him a happy birthday on his birthday. So Atlas arrived with a bang.
(Plaintiff's Exhibit Number 57 was introduced.)
Q. (By Mr. Cain) Okay. So Plaintiff's Exhibit 57. This is a still shot from your piece; correct?
A. Correct.
Q. And is this Professor Halderman?
A. It appears to be.
Q. And I think I have -- you'll just have to pardon me, because I'm my own paralegal, and I'm not very good at it. Let me see if I have -- if I can get to the piece

itself.
A. Well, you always had the A/C job to get to.
Q. There you go.
I'm just going to see if we can get to the part with Professor Halderman. It was pretty early on in this piece. I'll start at 2:09 in the piece.
(The video segment was played.)
Q. (By Mr. Cain) That's Dr. Coomer there, is it not?
A. It is.
Q. So let me ask you a couple of things about that -- that short segment.
I guess, going reverse, you mentioned that Dominion was a Canadian company. Have you now subsequently learned that Dominion, while it had an office in Canada, is actually a company that is formed and is a domestic U.S. company?
MR. RHODES: I'm going to object to the question and the term that, quote, "Dominion," closed quote, is vague and ambiguous. Depends on which Dominion you're talking about, Mr. Cain.
MR. CAIN: All right. Well, I'll rephrase that.
Q. (By Mr. Cain) Dominion Voting Systems is a U.S. company, is it not?
MR. RHODES: Same objection. There's more than

one Dominion Voting Systems.
MR. CAIN: Okay. Well, I think she can answer what her understanding is.
Q. (By Mr. Cain) If there's a distinction you want to make, you can make it, Ms. Rion.
A. Mr. Cain, my understanding is that Dominion Voting Systems was founded in Canada.
Q. And that's based on what?
A. Based, I believe, on Dominion Voting Systems' company profile. I -- I don't recall exactly, but I remember reading that they were founded in Canada.
Q. Well, they may have been founded. I'm not -- I'm not going to argue with you in terms of the timing of that.
But as of the election in 2020, it was a domestic U.S. company, was it not?
MR. RHODES: Same objection.
A. I -- I don't know if I would agree with that.
Q. (By Mr. Cain) And this is based on -- I know you referenced it, but is there some document that you're thinking of that you relied on when you made that statement?
A. I believe I saw articles of incorporation showing that Dominion Voting Systems was founded in Canada. They may have offices in Denver. They may have

offices, you know, in Antarctica. But that does not make them an Antarctic company.

I don't think that -- just because you have offices somewhere does not mean you were founded there.

Q. Well, for sure. I mean, Apple has an office in China. They're not a Chinese company; right?

A. Exactly. And it was founded in the West. So I think that's the distinction.

Q. Okay. And you -- you obviously saw Dominion's web page, because I think you produced that to us, where they identify the fact that they are not a Canadian company at present; true?

A. Yes. I used that page, I believe, in my "Dominion-izing the Vote" several times. I referenced it several times.

Q. Yeah. And we'll look at that in a minute.

I just want to make sure I understand where you -- where you -- what you were relying on when you made that particular statement

And what you're saying, as I -- as I appreciate it, is the original articles of incorporation of a Dominion entity, you reviewed prior to this report, and that's what you were basing this on; true?

A. Yes.

Q. You also said in that segment that we looked at

when you were showing Mr. Halderman that to -- to "ignore that." You used the term, "You can ignore that."

Can you tell me why you said that in this piece?

A. Yes.

That -- that was clearly a tongue-in-cheek comment meant to add to the -- I guess, the flow of the piece. I occasionally include tongue-in-cheek comments in my reporting.

Q. Okay. Well, I'm not the most humorous person in the world, so I didn't quite get it, which is why I asked question.

You showed Mr. Halderman in the piece, and then you said, "Ignore that," and then you went on to Dominion Voting Systems. So what's tongue-in-cheek about that?

A. I think that most viewing it might understand that as being ironic. It's clearly a statement from Professor Halderman that is highly relevant to the conversation.

But we are asked by mainstream media or large entities to ignore important statements from experts like Professor Halderman. So it was a statement in irony.

Q. I see.

And the importance, in your mind, here was that there are potential vulnerabilities in these -- in the

voting systems, and you wanted to make that clear; right?

A. Absolutely.

Q. All right. And you want to make it clear, also, to the audience -- and did in this piece -- that if there's important and relevant information concerning these vulnerabilities, you were trying to document that and educate your listeners and viewers; true?

A. I would say that's fair, yes.

Q. All right.

And in terms of -- sort of, a 30,000-foot overview of this piece, are there areas that you can cite us to where you identified, sort of, the other side of that -- that particular issue? And I'm talking about vulnerabilities.

It's one thing for there to be potential vulnerabilities. It's another thing, I think you would agree with me, for those vulnerabilities to actually be -- I'm struggling with the word -- but, essentially, utilized to rig the election. Those are two different concepts; right?

A. Not necessarily, not in this context, I don't believe.

We were citing documents from Dominion Voting Systems, their own user guides, that, in those user guides, there were some vulnerabilities that

penetration testers easily were identifying.

So I don't think that's a fair statement. I think that there were confirmable vulnerabilities in these machines, and they were being highlighted in our report.

Q. Okay. And, again, from -- you consider yourself a journalist; correct?

A. Yes.

Q. And I wasn't being pejorative on that. I just want to make sure that we're on the same page.

Do you actually have -- prior to coming to OAN, did you have some experience in journalism as a reporter?

A. None whatsoever. I had a degree in international relations, and that was my -- my educational background.

But -- well, in fairness, actually, the one journalistic course I ever took at my school, at Harvard University, was under Professor Allan Ryan. We did a course on journalism in the Fourth Estate. And I wrote the top paper. I was the top student in that course.

He was a rather famous attorney in D.C. and in Cambridge. That's about the only journalism formal education that I have had. But I believe my international relations background is sufficient for what I'm doing.

Q. Well, I'm just -- I'm just trying to get the experience. And it's fair to say you took one course when

you were getting your degree in international relations at Harvard by Professor Ryan, but you didn't have any actual experience in the field working as a journalist before coming to OAN; is that true?

A. No. No experience beforehand.

MR. CAIN: Rebecca, let's mark another exhibit from my private folder: 10-C. It starts 10-C, Expert Statement.

MS. DOMINGUEZ: Yes, sir.

Q. (By Mr. Cain) Can I ask, while she's doing that, if you didn't have experience as a journalist, how did you come to be hired by OAN?

A. I was recruited. I was at an event in D.C., and I was talking as -- as one does in D.C., talking to someone. And one thing led to another. I was invited to the OAN studio, and I was called on to do a screen test.

I met with Charles Herring. He interviewed me, reviewed my background, and hired me from there about two years ago.

Q. So you went from -- when you were originally hired, what were you hired to do?

A. I was hired to be the weekend White House correspondent and to -- outside of that weekend, to spend about three days doing regular reporting out of the D.C. bureau.

Q. Since you were new to the industry, did OAN supply you with information concerning journalistic standards of the news organization?

A. I don't remember that as much as I remember the mentorship that I received from my bureau chief, John Hines, and from our invest- -- our chief investigative reporter Neil McCabe.

They were -- they were my mentors, and they thought me everything, I think, I needed to know to get started in the -- in the news business.

Q. Okay. So fair to say you had, essentially, on-the-job training by John Hines and Neil McCabe was part of your mentoring to become what you are now?

A. Yes. But I wouldn't want to wish them -- wish on them the full responsibility. But, yes, they were my mentors, and they taught me what I needed to know.

Q. But aside from that mentoring, my question was geared towards the company actually supplying its journalists with either journalistic standards in writing or ethical standards for reporting.

And is it fair, then, to say that you never received that type of information from OAN?

A. No, not fair at all. I think I received a lot of guidance, in terms of just candid guidance on the job.

And that either came from my D.C. bureau, and

sometimes it came from my San Diego bureau, the San Diego side, where I would put reports together, and they might say, Here are some tidbits or hints and clues how to do this right.

I received a lot of guidance at the very beginning from a variety of sources at OAN.

Q. You and I are talking past each other.

My question was -- some news organizations actually have written standards for their journalists in terms of fact checking, in terms of vetting sources, in terms of ethical responsibilities. And that's reduced -- some put them on their website. Some put them in a -- in little booklet that they give out.

So it's a set of practices that the news organization expects their journalists to abide by.

So putting aside what you told me about mentoring -- I get that -- is there anything that you received that would meet that definition I just gave you?

A. Verbal training, I would say. I think that's a fair way to say it.

Q. Now, in the reading that you did -- let me back up.

Can we agree that the "Dominion-izing the Vote" piece was first broadcast on November 21st of 2020?

A. I believe so, yes.

Q. Okay. And when I took Mr. Herring's deposition, the report was still available on YouTube. Do you know whether it's been taken down since his deposition?

A. No. I believe the report you're referring to is the -- the report that was shared by the Donald J. Trump YouTube page, and we had nothing to do with their posting that report. And I believe it is still up today.

Q. Okay. I did a search the other day, and I couldn't find it. But that doesn't mean it's still there.

As far as you're concerned, it's still available through that page; true?

A. At last I have seen, yes.

Q. Okay.

I'm going to show you what's been marked as Plaintiffs Exhibit 58. I'm going to share my screen again.

(Plaintiff's Exhibit Number 58 was introduced.)

Q. (By Mr. Cain) So this is dated November 16th of 2020: "Scientists say no credible evidence of computer fraud in the 2020 election outcome, but policymakers must work with experts to improve confidence."

And it's, obviously, Plaintiff's Exhibit 58. It's a short document, and it's signed.

Now, in terms of this particular document, have you seen this before, Ms. Rion?

A. I don't believe I have seen this. But I've heard of the pushback from various sources saying that the election was perfect, and there was no chance for it -- for it being vulnerable, all of a sudden, in 2020.
Q. Okay. So let's break that down a little bit.
The first question was, had you seen this document before -- before I showed it to you. And I think your answer to that question is, no, you have not?
A. No, I have not seen this particular document.
Q. But you certainly -- it made news, and you certainly would have heard of this document being circulated on or around November 16 of 2020; right?
A. I don't remember. But I -- I know that the sentiment was certainly discussed as far as individuals who wanted to convince the public that our elections were perfect.
Q. And that's how you're characterizing this particular document, as the attempt to characterize the election as perfect?
A. I'm only judging it based on the headline that you've -- you've provided here. I'm assuming that this is "Scientists say no credible evidence of computer fraud in the 2020 election outcome, but policymakers must work with experts to improve confidence."
That was a sentiment that, I think, news

organizations affiliated with the left would push as well. We were -- we were simply questioning this logic, saying that the election was questionable in 2016, but suddenly perfect in 2020. So that's -- that was our position.
Q. All right. Well, you talked about vulnerabilities. And that's -- that certainly was the subject of -- at least one of the subjects of your piece: potential vulnerabilities in the system; right?
A. Correct.
Q. All right. And here you have a group of 59 election experts, including Matt Blaze, who -- whose research you found to be credible -- and also including Professor Halderman, who was on the piece itself, at least in part, issuing this statement in November 16th of 2020.
Now, why didn't you consider this report as part of your piece?
MR. ARRINGTON: Object to form. Identified as Barry Arrington.
A. I don't -- again, as in the other report I believe you showed us, I don't under- -- I don't know who was responsible for what parts of this report.
But I was relying on the experts that you just named having identified known vulnerabilities in our election system, and those claims, I don't think they were retracting. They're not retracting their identifying

known vulnerabilities in our election system in this statement.
Q. (By Mr. Cain) Okay. Some we can agree, then, if you look at the statement -- it's fairly short -- it starts, "We are specialists in election security, having studied this, security of voting machines, voting systems, and technology used for government elections for decades.
"We and other scientists have warned for many years that there are security weaknesses in the voting systems and have advocated that election systems be better secured against malicious attack." And it goes on to talk about that.
So that -- that's a statement, I think, that you and I can agree on; correct?
A. Correct.
Q. All right. Now the second -- the next paragraph goes on to say, however, quote, "Anyone asserting that a U.S. election was rigged is making an extraordinary claim, one that must be supported by persuasive and verifiable evidence. Merely citing to the existence of technical flaws does not establish that an attack occurred, much less that it altered an election outcome. It is simply speculation."
Do you agree with that statement?
A. I don't think it's extraordinary to say that

there were some massive vulnerabilities in our system, and that there are still questions that we pose about our election system as it stands today.
But after the "extraordinary claim," I agree that all -- all statements should be backed by -- by reasonable facts and evidence, and that's what we used in our report.
Q. Well, as you sit here today, you obviously are aware of no persuasive and verifiable evidence that the election was actually rigged; true?
MR. REAGOR: Object to form.
A. I disagree with that statement.
Q. (By Mr. Cain) All right. Tell me what persuasive and verifiable evidence you have that you can share with us here today that the 2020 presidential election was rigged.
A. Off the top --
MR. REAGOR: Object to form.
A. Off the top of my head, I mean, there are dozens of stories that I can point you to. But, at present, I don't want to give false details.
But if you look at the Arizona election, for instance, that election was won by a margin of about 10,000. And to this day, there are questions about the voter rolls that were involved in that election.

There were well over 10,000 votes that were involved in the Arizona presidential election that should not have been qualified to vote in that election.

So you could compare that -- the voter rolls from these states with the margins of victory for these states, and I think that's one example that I can give you at this time.

Q. (By Mr. Cain) Okay. If you think of any others during the course of your deposition, flag those for me, and we can talk about them.

But you're talking about voter roll issues in Maricopa County as being some evidence that there was rigging of the 2020 presidential election?

A. But, Charlie, this is also still very much in question. I don't think we can stand here today and say with certainty that the election in 2020 was infallible; it was perfect.

So I don't think that it's fair to come to a conclusion even now. There's an audit that's still ongoing down in Arizona in Maricopa County, and now audits that are starting to crop up in Wisconsin, potentially in Georgia and Pennsylvania, indicating that there are still lingering questions that need to be answered about our elections and the vulnerabilities that are posed in them.

Q. You keep using the term, Ms. Rion, "perfect."

You've said that now three or four times. Who is it that you're referring to as indicating that the election in 2020 was, quote, "perfect?"

A. I am paraphrasing, Charlie.

So in this case, it's just -- you have scientists saying no credible evidence of computer fraud. I think that's a big statement considering that many of these individuals were also involved in years of hackathons showing that there were vulnerabilities that could be easily exploited undetected.

For example, the professor you cited down here, J. Alex Halderman, he himself was able to hack into these machines in a period of a few hours, and he was able to do so undetected.

So it seems rather extraordinary to say that there is no -- there is no capacity for -- for vulnerability here.

Q. I don't think -- I think we've talking about two different things: capacity for vulnerability and actual exploits. And we'll talk about that in a little more detail.

A. Again, that's still in question. Right now, there are audits taking place trying to answer that question.

Q. Yeah. I hear what you're saying in terms of

ongoing audits. The one you referred to is a -- well, let me ask you about the Maricopa County audit.

Are you participating in that audit, either through a financial investment or through your reporting?

A. I've certainly reported on it. I don't -- I don't know what you mean by financial involvement.

Q. Yeah. That's a lawyer word for -- are you -- are you paying any money in support of that audit, contributing to a fund?

A. I personally am not doing that.

Q. Are you aware of anyone at OAN contributing to that?

A. There's -- with my colleague, Christina Bobb -- she is the CEO of Voices and Votes. This is an organization has been raising funds to help provide for audit needs in Arizona or Maricopa County.

As far as being personally compensated, none of us have been personally recompensated. All donations have been raised through Voices and Votes have gone towards -- towards the audit in Maricopa County.

Q. Have you personally contributed to Voices and Votes in support of that audit?

A. I have not in terms of monetary; but in terms of time, I have certainly contributed time and reportage on it.

Q. When you say "time," what do you mean by that?

A. I am the marketing director for Voices and Votes, providing some -- I'm providing the email updates for individuals who are subscribed to Voices and Votes.

Q. And what is your -- is -- is -- are we getting feedback from someone else? I keep hearing --

A. I think we heard someone laughing the background, and my newborn is starting to rustle.

Q. Okay. Let's power through until we can't.

Tell me what your role is as marketing director. What do you do object a day-to-day or weekly or monthly basis?

A. I provide email updates.

Q. Is that it?

A. Yes.

Q. And then Ms. Bobb, she's a -- is she also a journalist for OAN?

A. She's a journalist, and she hosts the opinion show on the weekends called Weekly Briefing based here in D.C.

Q. And you don't host an opinion show. Your reporting is fact-based; true?

A. I don't think I can answer that with a yes or no. Sometimes I add -- as you saw in my

"Dominion-izing the Vote," sometimes I add tongue-in-cheek statements which are categorized as opinion.

But for the most part, I report on fact-based stories with a dash of tongue-in-cheek, sometimes, in my OAN Investigates specials.

Q. Let's circle back to the exhibit, since still have it up on the screen.

We were talking about exploits versus actual vulnerabilities. The next paragraph of this statement from the election security experts starts, "The presence of security weaknesses in election infrastructure does not by itself tell us that any election has actually been compromised.

"Technical, physical, and procedural safeguards complicate the task of maliciously exploiting election systems, as does monitoring of likely adversaries by law enforcement and the intelligence community. Altering an election outcome involves more than simply the existence of technical vulnerabilities."

Do you agree with that statement?

A. I do. I agree with that. And I believe that we, as a network, agree with showing these vulnerabilities and reporting on it. So that's what we did -- that's what we had done with "Dominion-izing the Vote."

Q. Well, it's fair to say that part of that report,

"Dominion-izing the Vote," is about Dr. Coomer; true?

A. A portion of it is about Dr. Coomer.

MR. RHODES: Charlie, Ms. Rion, I -- I hear Atlas. Do we need take a break?

MR. CAIN: Yeah. I -- I -- we can't have that. It's not going to be okay to have Atlas in the background during this. So let's go off the record.

THE VIDEOGRAPHER: Going off the record. The time is 12:54.

(Recess from 12:54 p.m. until 1:06 p.m.)

THE VIDEOGRAPHER: We're back on the record. The time is 1:06.

Q. (By Mr. Cain) Okay. We were talking about Exhibit 58 to your deposition, Ms. Rion.

The next paragraph that I haven't addressed is the one that starts "We are aware":

"We are aware of alarming assertions being made that the 2020 election was rigged by exploiting technical vulnerabilities. However, in every case of which we are aware, these claims either have been unsubstantiated or are technically incoherent.

"To our collective knowledge, no credible evidence has been put forth that supports a conclusion that the 2020 election and outcome in any state has been altered through technical compromise."

Now, in your report, "Dominion-izing the Vote," a claim is being made that Dr. Coomer was in a position to exploit technical vulnerabilities in the system; true?

A. I believe so.

Q. And your report indicates that Dr. Coomer, in fact, boasted about rigging the election himself; true?

A. As relayed to us through Joe Oltmann.

Q. Right. You aired Mr. Oltmann's statements about that episode; correct?

A. Correct. We interviewed Joe Oltmann for the piece.

Q. All right.

Now, in terms of Dr. Coomer's ability to exploit technical vulnerabilities in the system, is there a basis, in your mind, for Dr. Coomer to actually do that as a practical matter?

A. When researching Dr. Coomer and his background, it was very clear to us that he had a very high level of expertise in voting systems, and especially at Dominion Voting Systems.

This was evidenced by the fact that I had found six -- six patents filed in Eric Coomer's name for Dominion Voting Systems, and an additional six applications as well, I believe, but multiple patents under Coomer's name, where he had not only a role, but it

seemed, with his name on the patent, he actually invented means to adjudicate ballots and adjudicate imagery that was going into these machines.

And in discussing with -- with experts who were look at the vulnerabilities of these machines, we knew that there were some vulnerabilities on the image adjudication side of things. And so this made sense to us as we were looking at Eric Coomer's background, his expertise, as confirmed by the U.S. patents he had under his name.

Q. Well, if -- you would agree with me, if -- if -- the implication from your story is that Dr. Coomer actually exploited technical vulnerabilities in the system; fair?

A. We posed that question, and we simply exposed the fact that he had this ability.

I don't -- I don't know that we said that he particularly did that. But we are exposing the fact that he had this means and the access and the expertise, and this is something that we were looking at as a story.

Q. Okay. Let's break those down, Ms. Rion.

The means -- what means were you exposing that Dr. Coomer had access to the system in order to exploit the security vulnerability?

A. Means in terms of his actual job title. He is

the head of secur- -- he is the vice president of security and strategy at Dominion Voting Systems.

Our research found that he was a representative for Dominion Voting Systems in some key states across the country in selling these systems.

He was very intimately involved, it seems, from the outside, with the operation of these machines, the design of certain elements of these systems, and representing them to states that were considering purchasing these systems.

Q. All right. Well, my question again, I think, was a little more specific as to what means were available to him in order to exploit a technical vulnerability in any of the swing states.

A. I think we did a fairly good job in our piece in showing that he had the access.

Now, as to the exact physical date and time in which he would have had the means to do this, I think that's a question for your client.

Q. Well, I think it's a question that needs to be answered about your piece. Because the suggestion is that he had the means, and he acted on that.

And my question to you is, give me your view of how he had the actual means to infiltrate and exploit a vulnerability in the system. I have not heard an answer

to that.

MR. REAGOR: Michael Reagor. Object to form.

A. Mr. Cain, if you look at -- I think it was in the DEF CON report -- I'm sorry. I'm citing the wrong document.

I think it's in the user guide itself of Dominion Voting Systems. In the user guides for Dominion Voting Systems, there are two manuals that I read in the research -- doing research for this piece. And in both manuals -- and I can't -- I don't know if I can cite the exact page numbers.

But in both manuals, there are ways in which an engineer can remotely access these machines and fix problems, to put it in layman's terms, with the system. If there were any -- any problems with the system, there are ways that a Dominion engineer either exclusively had to access these machines or could remotely do so.

That's one way. I'm not saying that is the way, but that is one possible way. And it's in Dominion Voting Machines' [sic] manual in their own words.

Q. Did you, as part of your reporting, come up with some evidence that there was remote access by either Dr. Coomer or anyone at Dominion Voting Systems in any of the battleground states during the election?

A. There's a point I'd like to highlight in

answering this question.

I believe Dr. Coomer was also head of engineering at Dominion before he became vice president of strategy and security.

So I think we were looking at those pieces, those facts, and the fact that he had these rabid, it seemed, very, very harsh feelings about the election, about Donald Trump. And he was -- he seemed to be someone who took his anger out into action by his Facebook posts.

So we were looking at those pieces and simply presenting them in our "Dominion-izing the Vote."

MR. CAIN: Objection. Nonresponsive.

Q. (By Mr. Cain) My question, Ms. Rion, was as to remote access. You raised that issue of the potential for remote access.

The question was, in your reporting, did you find any evidence that Dr. Coomer actually had remote access to any machine in a battleground state --

A. I think --

Q. Let me finish.

-- and actually acted upon that? Do you know of any evidence of that?

A. We never -- Mr. Cain, I don't think we ever boasted of having that evidence. We simply highlighted the fact that Dr. Coomer had the particular expertise that

he had; that he had the position that he had at Dominion Voting Systems, this high-level position.

He had the -- the motive. It seemed he was very motivated to not -- to ensure that Donald Trump was not elected, it seemed, through his Facebook posts. We were simply highlighting that fact.

So I don't think we were giving a name, a date, and a place, because, obviously, we're not God. We're not everywhere at once, so we couldn't see any of this.

But Dr. Coomer had the means; he had the expertise; and I think we highlighted that fairly well in our piece.

MR. CAIN: Objection. Nonresponsive.

Q. (By Mr. Cain) The question that you need to answer is, do you -- are you aware of any evidence that Dr. Coomer actually accessed any of the voting machines in the battleground states remotely during the election? Yes or no?

A. No.

Q. When looking at Exhibit 58, what I'm trying to gauge, Ms. Rion, is the likelihood or probability that Dr. Coomer could exploit technical vulnerabilities. Because, as you've said now many times, you were highlighting the fact that he had the means and the access to do so.

So with that in mind, I want a probable scenario under which Dr. Coomer could affect the election outcome in 2020. What probable scenario can you identify for the Court that would support that notion?

A. There are many scenarios. I mean I can't, obviously, list all of them.

But one that comes immediately to mind is -- and it was previously highlighted in my special -- was the fact that Dr. Coomer had patents in image adjudication, ballot adjudication, image cast systems -- I don't know the exact terminology. But it was -- he had several patents in ballot adjudication using the images of ballots.

We know that in Arizona, in Maricopa County, for example, ballots were printed on two sides in the vast majority of precincts. It may have been all precincts, but the vast majority of precincts had double-sided ballot printing.

And we also know that there were Sharpie pens used that -- Dominion Voting Systems itself says Sharpie pens were not an issue, but we know -- we have seen pictures from voters in Arizona showing that the double-sided ballots were bleeding through when they used Sharpie pens.

That's relevant in the following sense: When

you're feeding a ballot into a machine, if the machine has its gamma settings adjusted so that it's extremely sensitive, there's a way for, for example, every single ballot in a given precinct to be set aside for adjudication.

Now, if, say, 2,000 ballots were set aside for adjudication here and there, and you combine those and you have, maybe, five or six precincts in Maricopa County where a couple thousand ballots were set aside for ballot adjudication because the image casting technology was used, and those ballots were set aside for someone to adjudicate, that's a vulnerability.

That's a possible way that a couple thousand votes here and there could have affected an entire state and, therefore, an entire election.

Again, I'm not a technical expert, but that's an overview of one of many scenarios in which, through nicks and cuts here and there, an entire election could be affected through these systems.

Q. Okay. Well, let's run with that one, since you mentioned it.

Is Dr. Coomer, to your knowledge, responsible for the design of the balloting in Maricopa County, or is that done by the county?

A. I don't know what his involvement in

Maricopa County is.

Q. Did Dr. Coomer, to your knowledge, calibrate settings on the devices in Maricopa County, as you refer to the gamma settings?

A. I don't know. But I know that he designed the system to help that system exist. And he was also -- he also had a presence -- Dr. Coomer had a presence in Arizona when he was, I guess, representing Dominion Voting Systems.

We have, I believe, video or documentation showing Dr. Coomer in Arizona discussing these systems and explaining these systems to -- to local officials.

So we have his presence in Arizona, his role in inventing a system for ballot adjudication. Those are just a couple of items that are notable.

MR. CAIN: Object as nonresponsive to everything after "I don't know."

Q. (By Mr. Cain) You don't know if Dr. Coomer had any direct role in controlling the gamma settings in Maricopa County; fair?

A. Fair. And again, I did not say that that's what he did. You asked me for an example, and I gave you one that, I think, is reasonable.

Q. Well, it's reasonable if -- if it's probable or if there's some likelihood that he had the ability to do

that. And that's why I'm asking you these questions.

Because in this report that we're looking at, or at least the statement, we're talking about something that is either simply speculation or there's some factual basis to it. So that's -- that's what we're exploring right now.

A. And again, I don't -- I have not read this entire document. But from what I've read, I see no mention of Dr. Coomer in this document and no mention of the fact that the election wasn't rigged.

So I -- I understand the relevance of this document, but I also think it's important to note those facts.

Q. Well, I don't -- we don't need to quibble over it, because the Court can read it.

But it says: "To our collective knowledge, no credible evidence has been put forth that supports a conclusion that the 2020 election outcome in any state has been altered through technical compromise."

That's a -- a fair reading of that, We've come to the conclusion there's no evidence that the election but rigged through technical means.

A. I think we can read that phrase, but also agree that it's not -- I don't think anyone can really say whether this statement is true or not. It still --

Q. Well, at least -- I'm sorry. I didn't mean to interrupt you.

You obviously don't consider yourself -- I know you've read up on some of these aspects, but I think you've stated you're not a -- an election expert. That's not your expertise; true?

A. Not an election expert.

Q. Correct?

A. Correct.

Q. All right. And so to the extent that you're reporting on this, you're relying on other experts to -- to explain the technical aspects of voting systems; fair?

A. Correct. And we would use voices that, obviously, would contradict this report. And I think that's newsworthy, and that's what we put out.

Q. Well, let me ask you this: I mean, if you're making the claim, as they say, that the election was rigged -- and you cited to Maricopa County --

A. I -- can I interrupt? May I interrupt?

Q. Yeah. Sure.

A. I never -- don't believe I've ever used the phrase "The election has been rigged."

Q. I see. Well, I don't mean to put words in your mouth.

I guess, let me ask this way. What I'm trying

to figure out -- if the implication -- well, let me -- let me start with that.

The implication from your report is that Dr. Coomer, as you put it, had the means and access to exploit the voting system software and hardware; fair?

A. That is one portion of my report. I think there's about 24 minutes or so of additional content that's not about Eric Coomer. But, yes.

Q. Okay. And I don't represent the rest of the folks on the video. I represent Dr. Coomer, which is why I'm asking about him.

What I need to understand, ma'am, is whether your -- your implication in your piece has some inherent probability that it could actually be true; right?

So we can speculate all day long about what Dr. Coomer could or couldn't do, but is there any theory that you can think of that makes it likely or probable that Dr. Coomer actually had access and did the things that you're suggesting?

MR. RHODES: Objection. I'm sorry. I thought you were finished. Are you finished, Charlie? I'm sorry.

MR. CAIN: Yes. "Anything," question mark, was the last one.

MR. ROGERS: Okay. Objection. Asked and answered several times.

Q. (By Mr. Cain) You can answer.

A. Would you repeat the question?

MR. CAIN: Sara?

THE REPORTER: Yes.

MR. CAIN: Oh. I'm sorry. I'm used to working with Bill Fredericks. So when I say, "Bill," he knows to read the question back under the circumstances.

THE REPORTER: No. I heard you. I just -- it's a long question, so I'm trying to figure out where to start.

(The reporter read back the last question.)

MR. RHODES: Objection. Asked and answered.

A. Yes. Absolutely. There's -- and I have answered this question.

I think that he had the means, the access, and he was physically in these states, as he was representing the Dominion Voting Systems.

There are -- the system is designed so that they can be remotely accessed. There's a number of scenarios. And so, yes, it's highly likely.

And that's how we represented this in our -- in our "Dominion-izing the Vote." We represented the facts. We represented Eric Coomer's own words, his title, his role at Dominion, his expertise, his battleground.

And you take all of these facts into account,

and most reasonable people who are watching will say that there is a likelihood this individual, with the sentiments, the anti-Trump sentiments that he had, would have been able to act upon them.

Q. (By Mr. Cain) You mention the remote access to the systems. Are you aware of any instance in any of the battleground states that -- that the systems were remotely accessed by Dominion employees?

A. I -- I don't know. But I think that when you look at the DEF CON reports showing these hackers accessing these machines and doing so undetected, that's -- that is also an answer.

There's a way that all of these machines could have been accessed. And it's possible that they were not detected, as proven by the DEF CON hack of -- Hackers Village.

Q. Which battleground states had machines with remote access capabilities?

A. I don't know that I can answer that question. I assume that these user guides were -- are describing Dominion Voting Systems as a whole.

So we're talking about anywhere Dominion Voting Systems using these manuals would have been, so Georgia, Arizona. I believe there are 20 states that Dominion Voting Systems was operating in, or at least

providing machines services for.
Q. I'm just asking about the battleground states. Which of the battleground states, if you know, had Dominion voting machines with remote access?
A. Well, again, assuming that these user guides are describing the machines that were in battleground states, Georgia -- I think every precinct in Georgia was using Dominion Voting Systems -- Arizona, Michigan.
These are battleground states that were using Dominion voting machines, assuming those user guides are accurately representing those machines.
Q. And did you produce the user guides that you're relying on?
MR. RHODES: Yes, we did.
Q. (By Mr. Cain) So in terms of your last response, which you said twice "assuming" these user guides or user manuals were applicable to these states, the user guides that you're mentioning are the ones that you provided to your counsel and have been produced to us?
A. Correct. And assuming that those user guides are accurate from Dominion Voting Systems; assuming they're not misrepresenting their own machines.
Q. Yeah. Well, you're not -- well, as you sit here that, kind of, begs the question: Do you know whether or not the guides misrepresent the actual machine

capabilities?
A. I don't. I assume that those user guides are accurately representing their own machines. I don't understand why they would not. I wouldn't know for certain.
Q. Okay. And then, kind of, going back -- and I know we've gotten in the weeds on some of the technical issues. But did your research turn up how the certification process was administered on a county-by-county basis in the battleground states?
A. I may have looked at that. I don't recall at this moment.
Q. Did your research --
A. You're saying -- I'm sorry. Can I understand your question?
You're saying the certification process from each of these states for Dominion Voting Systems?
Q. Yes, ma'am.
A. Oh, yes.
So I looked at -- again, I think I mentioned this at the top of our conversation. But the secretaries of states for Texas, Pennsylvania, I believe -- and I don't remember if it was Arizona or another state. But I certainly know that I looked at the documents out of the secretaries of state's offices from Texas and

Pennsylvania.
And in those certification, I guess, documents that they had, they -- Texas listed vulnerabilities that caused the state of Texas to not purchase Dominion machines for their voting -- for their precincts.
Pennsylvania, I think, did use Dominion voting machines. And I looked at their documents as to why they certified Dominion.
Q. Okay. So you are aware, then, and were at the time of this report that the states have their own certification process that is a condition preceding to this -- the voting systems actually being used in their jurisdiction?
A. Yes.
Q. Okay. And likewise -- well, not "likewise," but going back to this issue of these gamma settings, did your research inform you on who actually has the ability to control those settings?
A. I -- again, I'm not an expert in this, but I'm sure a hacker could answer this question. I don't know that.
I know that there -- the Texas document -- the Texas Secretary of State's certification, I guess, decline letter listed how there were vulnerabilities in the USB drive -- not necessarily the image, but the USB drive --

and how that was a gaping vulnerability to an election system.
That's another example of one way that ballots, en masse, could be tampered with. But I think that answers your question.
Q. Okay. Well, we may swing back into that for a second, but I need to move on to a few other things that I think I need to know about.
Remember, we talked about you putting this piece together in D.C. You mentioned that you -- you wrote the piece. And I asked you, Did anybody else edit the actual portion of it? And I think your answer was no. It was, essentially, your baby, as we said; true?
A. True.
Q. Okay.
A. And I would be -- again, I discussed the -- I discussed my piece with Charles Herring and, I think, John Hines occasionally.
But just over the course of discussing the progress of the piece, discussing details of it -- I don't remember all of those conversations, but I know that I discussed with Charles Herring portions of the piece before it went to air. And I know that he watched the whole thing before it went to air.
Q. Okay. Did you have any discussions with

Brandon Gadow about this piece?
A. Only technical ones, that I remember. He's -- he would edit in San Diego, so we would send -- I would send him progress reports: Hey, my editor is 75 percent of the way there, or he's almost finished, or we should be submitting this piece in a few hours. Those are the extent, I believe, that I would have discussed with Brandon Gadow.
Q. Okay. These progress reports, are those in the form of an email that you would send to him?
A. No. I think we would be chatting on the phone.
Q. Okay. Help me with -- I'm not in the news business. How would Mr. Gadow be in a position to edit your report over the phone? Would you just read a section to him, or how would that work?
A. No. When I -- when I say "edit" -- I'm sorry. I didn't clarify. When I said "edit," I believe what Brandon is doing is just, you know, he's listening to the piece. He's watching the piece.
He would ensure that, technically, it had all the sound elements ready to broadcast. I think he's largely in charge of the technical side of ensuring that our pieces go out broadcast-ready.
Q. Okay. Well, that's -- I -- I get the technical part. What I'm trying to get to is, did he have some

editorial content to this particular piece, if you know one way or the other? And did he have any fact-checking role?
A. I believe that all of our OAN Investigates pieces go through a fact-checking process. I don't know what that is.
I've never actually met Brandon. But I know that several eyes do the fact-checking, including Charles Herring and Brandon Gadow. But I don't know what that process is.
I know that Brandon is a technical editor, and he edits the technical aspects and listens to the entire piece from beginning to end to ensure that it's broadcast-ready. And whether that's editorial or technical, I can't say for all of his work descriptions.
But as far as this piece is concerned, I recall only technical elements being edited.
Q. But as you sit here, you have no personal knowledge of any fact-checking that was done in San Diego relating to this piece; true?
A. There was plenty of fact-checking in San Diego. I don't know -- I can't speak to exactly what all they did, but there's always fact-checking going on, on both sides, both bureaus.
Q. Ma'am, I was asking you about your personal

knowledge. So let's limit it to that.
You said there's always fact-checking going on. That's not what I was asking.
In this piece, do you have any personal knowledge --
A. Yes. In my discussion with Charles Herring, I mean, we would talk about trying to find, for example -- one example -- and this is one of many for this piece, including -- we would -- I would talk with Charles Herring about the various interviewees or -- or elements of the story.
One example is when Charles Herring called me and said, Look. This -- this Eric Coomer story is interesting. Can you find Eric Coomer? Please try and contact him. Can we verify this is him?
So these are the kinds of efforts that I would then execute. And then Charles Herring, I know, was doing his own research into this, and he was very interested in this particular story.
So I know that Charles Herring did a lot of -- a lot of research into this. I did research into this.
I know we had several producers in San Diego, independently of my knowledge -- I've now learned later that they were also doing deep-dive verification of the Eric Coomer story and Joe Oltmann. They were collecting

information, as far as I know, from what I've seen in these past -- in these past depositions.
Q. Okay. I heard what you said about Mr. Herring. My question was personal knowledge about fact-checking. You gave me that example.
Then you just said you know that there were deep-dive verifications of this story. You know that for a fact. So tell me about that.
A. Documents that, I think, we produced to --
Q. Ma'am -- ma'am, please. Sara's going to get upset if we talk over each other.
What information can you give me to support that statement that there was people doing a deep-dive verification of the information in this story?
A. I believe you presented one of our own emails, an email sent to OAN where information was being shared about -- about Eric Coomer. And then one of our producers -- I don't remember which one -- started looking into this story.
Q. Taylor, maybe? Or Scott? I can't recall --
A. Yes. Something like that. And they started looking into it.
I don't -- I can't speak to their research. I wasn't there.
Q. But you said -- I'm sorry.

A. They clearly were pursuing an investigation into the story before I even reached the story, actually.
Q. Okay. And I don't want you to speculate. That's why I'm asking you from your personal knowledge, meaning you saw it, you were involved in the conversation, you know for a fact because you witnessed it.
Other than the statements about Charles Herring and the interactions you had, what personal knowledge do you have that your story was fact-checked and verified in San Diego?
A. I think I answered that question with Charles. Charles and I would have those conversations about various piece -- elements of the story, and we would verify it.
Q. Who was your news director, or the news director, at OAN in November of 2020?
A. You mean -- we have a news director in San Diego, and we have a bureau chief in D.C. I don't know -- I'm unclear what your question is.
Q. I asked who was the news director.
A. The news director in San Diego is Lindsay Oakley. And our bureau chief in D.C. is John Hines.
Q. Okay. And is Ms. Oakley still at OAN?
A. As far as I know.
Q. Okay. And in terms of structure, the frontline

producers in San Diego would report to Ms. Oakley as the news director; is that true?
A. I believe so. Again, I'm -- I haven't even stepped foot in the San Diego headquarters, so I don't know the exact details. But I believe that is the structure.
Q. Okay. What -- what role, if any, did the news director at OAN have in producing this piece?
A. I don't recall ever discussing this piece with Lindsay Oakley.
Q. How about Robert Herring Sr.? We talked about Charles Herring. What role did he have, if any?
A. I don't know. I mean, we discussed stories amongst one another. And sometimes Mr. -- Robert Herring is on conference calls. So he may have been on conference calls sometimes when I was discussing this story with Charles Herring.
So I'm -- I cannot answer, with confidence, that question.
Q. Mr. Herring, Charles Herring, testified that Pearson Sharp may have had a role in this story. What role, if any, are you aware of him having in the production of this report?
A. I'm aware that he was reporting on general election vulnerabilities. He did not -- we did not

collaborate for "Dominion-izing the Vote."
Q. Okay. And then, you had mentioned early on, again -- what I want to turn you to now is your sources for this reporting.
You mentioned some -- I don't know if you'd call them white-hat hackers, but hackers that you talked to. Can you identify who you talked to that fits that bill?
MR. RHODES: On behalf of Ms. Rion, we object to the identity -- providing the identity of these hackers on the grounds of the reporter's privilege.
MR. CAIN: Okay. Well, I think that has been ruled on and dispensed with by Judge Moses. So --
MR. ROGERS: Judge Moses has never even heard of the idea that there were hackers who provided information not about Dr. Coomer whatsoever. And so I disagree vehemently with you that she has already ruled on that.
MR. CAIN: Okay. Well, again, you and I can agree to disagree.
Q. (By Mr. Cain) If -- let's take it this way, Ms. Rion. Did you identify and interview hackers in connection with your investigation and research for "Dominion-izing the Vote"?
A. The one that I can comfortably say on camera to you, Mr. Cain, is Ron Watkins. I interviewed Mr. Watkins. He is in my piece. He shows his face on camera.

He is a systems penetration tester, which is, I guess, a long-form or technical way of saying you're, kind of, a hacker. You're someone who goes through systems and tests out their vulnerabilities.
Q. Okay. And is this the only person that you can think of that fits that category when you gave me the testimony earlier?
A. I have other sources, but I don't -- they -- by nature of what they do, they -- I don't want to reveal their identities.
Q. Well, were these sources that you used in this piece in connection with investigating and researching for this piece?
A. In my discussions to verify, for example, what Ron Watkins was telling me about the vulnerabilities he was identifying from a technical side, I may have discussed with these individuals -- tried to verify that what he was saying was correct or was sound or reasonable from a technical standpoint.
Q. Well, that's -- that's a "may".
Did you get advice or information from other hackers that what Mr. Watkins was saying in your piece was technically sound, as you put it?
A. Yes. They -- not in writing. I would discuss this with them. But in my discussions, they would affirm

or, at least, put a thumb of approval on the analysis that Ron Watkins had provided to us at the time.

Q. Okay. And -- and so your piece, you talk about Dr. Coomer having the means and access to exploiting technical vulnerabilities; right?

A. Yes.

Q. That's -- that's step one.

Step two was you had Ron Watkins explaining his view on the technical vulnerabilities; correct?

A. Correct.

Q. And then step three is you had other sources that were grading Ron Watkins' paper, for lack of a better word, in terms of whether or not his theory was credible; fair?

A. "Theories" plural. He had several theories about the identified vulnerabilities in Dominion systems. Fair.

Q. Okay. And you're refusing, based on the assertion of privilege, to identify these individuals that you consulted with; true?

A. Absolutely.

Q. And you're refusing to divulge the substance of any conversations you had with these individuals?

A. I can -- I'm comfortable giving you the general substance that I can recall.

I -- when -- when confronting a story of this kind of technical depth, if you will, it's, of course, important to not be -- not just be pulling from one source when it comes to that technical expertise.

And so it is -- it is incumbent upon my own understanding of this explanation that I was receiving from Ron Watkins to ensure that I was getting a sanity check from others in his field, and that's what I was doing.

Q. Okay. But as you sit here, can you recall anything specific concerning the technical verification of Ron Watkins' statements on your report?

A. Yes. He goes through several vulnerabilities, including the gam- -- adjust- -- the adjustment of the gamma settings on the machines and the accessibility of the USB portals; the fact that it was -- it was fairly easy for these machines to access the internet and thereby expose the entire precinct or system to vulnerabilities.

The fact that some of these machines were operating off of one key, and that key controlled an entire precinct. These were verified by myself.

Q. Okay. We may be talking past each other again.

I think you were answering as it relates to what Mr. Watkins said in your piece, and my question was what -- what -- with these other sources, what technical

verification did they provide to you that you can recall that supported Mr. Watkins on your show?

A. I think I just listed them.

Those -- the capacity for these systems to be vulnerable in the ways that I just listed were confirmed by my other sources in discussing Ron Watkins' analysis.

Q. How many other sources did you contact that you're claiming a privilege of? How many, like, total number of people?

A. At this time, I'll say two. There may have been three, but I think I can comfortably say two.

Q. And these individuals reviewed your interview of Mr. Watkins prior to it going to air?

A. I would discuss with these sources what I was hearing. I would, you know, discuss the vulnerabilities that Ron Watkins listed, and I would relay that to my sources, and they would converse with me about those -- those findings from Mr. Watkins.

Q. Okay. So we've got Mr. Watkins who -- who was one of your sources who ended up on the -- on the program. We've got these other unnamed individuals. Let's just -- let's just complete the list.

You interviewed Mr. Oltmann, and he's one of your sources; right?

A. Yes.

Q. You interviewed Sidney Powell; is that -- in connection with this?

A. I tried to interview Sidney Powell, but she did not appear in my special. I did not interview her, ultimately.

Q. Well, I think she may have appeared just on a video cut, but not -- no any substance; right?

A. Correct. I used a press conference she appeared in, in lieu of my interview. We had anticipated having Sidney Powell interviewed in this piece, but it did not work out. She just never showed up for us.

Q. The other sources -- Rudy Giuliani -- was he one for this piece?

A. For this piece -- not about Dr. Coomer, but about election vulnerabilities in general.

Q. Anybody else that you used as a source for the segment that related to Dr. Coomer?

A. I listened to Michelle Malkin's interview of Joe Oltmann. I interviewed Joe Oltmann. And then as far as sources, we used Eric Coomer's own words.

Q. Well, okay. When you say "Eric Coomer's own words," he's not interviewed for this piece; right?

A. No. But he was posting on Facebook, and we assume that is in his own words. That's what I mean when I say "in his own words," he was posting on Facebook.

We were looking at about 80 screenshots provided to us by Joe Oltmann. We had no reason to believe that those screenshots were not of Dr. Coomer of Dominion, and we sourced our report on Eric Coomer's own words.

Q. Okay. Well, I -- I misunderstood, then.

I -- part of the statements that are attributed to Dr. Coomer are from Mr. Oltmann about the Antifa conference call; right?

A. I believe it's just one statement. The vast majority of the statements we pull from are from Eric Coomer's Facebook postings, I believe.

Q. Well, we don't need to weigh the number.

The statement in question that you actually put on Twitter comes through Mr. Oltmann. It's not -- you can't confirm that it's actually Dr. Coomer --

A. It comes through Mr. Oltmann. That's correct.

Q. Right. So you -- you are not and we're not in a position to independently confirm those are actually Dr. Coomer's statements; true?

A. We confirmed it in the sense that we were looking at the language that was used, the context of the setting, the group that the call was made in or the group that the call was, and matching that up with Dr. Coomer.

Q. Okay. But as you sit here -- I hear what -- what you've said. But you're not in a position to

confirm, though, that it actually was Dr. Coomer; fair?

A. I think it's unreasonable to assume that he -- that wasn't Dr. Coomer, especially when you look at the syntax, the -- the place setting, and the group it was in, and the fact that the statement was "Eric from Dominion."

The newsworthy side of this entire story was not so much the notes or the phone call; but the newsworthy element that we put out was sparked by notes, was sparked by Joe Oltmann's testimony.

But that, ultimately, wasn't gist of our story about Eric Coomer. The gist of our story about Eric Coomer was the fact that he had background, a technical battleground, with Dominion Voting Systems. He was a high-level individual at Dominion Voting Systems.

His own Facebook postings showed that he had -- he was very motivated and very anti-Trump in his sentiments, and he seemed to be acting upon those sentiments.

Those were the newsworthy elements of our reporting on Eric Coomer. And I think that stands today.

Q. Respectfully, I'm going to object as nonresponsive, because that did not answer my question.

But we also have Atlas crying again. So I think, maybe -- we need to get a clean record. Let's go off.

THE VIDEOGRAPHER: Going off the record. The time is 1:55.

(Recess from 1:55 p.m. until 2:08 p.m.)

THE VIDEOGRAPHER: We're back on the record. The time is 2:08.

Q. (By Mr. Cain) Let's talk a little bit more about corroboration relating to some statements attributed to my client.

I'm going to share my screen. Give me a moment.

This was previously marked as Exhibit 33. And this is -- this is a tweet you sent out -- see if I can get the date -- November 17th. Is that -- is that true?

A. It appears so, yes.

Q. Okay. And we were talking about the gist of your reporting on Dr. Coomer. In this particular tweet, you chose to cite to a quote from Dr. Coomer from your piece; correct?

A. I used the hashtag #Eric Coomer, which, by this time, I think his story was trending for about three days on Twitter and social media. So I used the hashtag #Eric Coomer, along with the phrase that everyone was using with that hashtag.

Q. Okay. And this phrase was something that was repeated in your -- in your interview of Mr. Oltmann from "Dominion-izing the Vote"; correct?

A. Yes, attributed to Dr. Coomer.

Q. Right.

So back to my -- my prior questions, other than what you testified to previously, what other corroboration, if any, do you have that Dr. Coomer actually made these statements, or this statement?

A. We were just matching up his -- his syntax, his Facebook posts, his sentiments on his Facebook posts, his title, his job title, and his education and background.

Q. Okay. And that's why I phrased my question "other than what you previously reported -- or testified to."

Is there anything else beyond that that you used to corroborate this statement was made by Dr. Coomer?

A. I think that -- I think I've stated my answer. The answer I just gave you, I think, is the answer.

Q. Okay. Thank you.

Obviously, there's no recording of this Antifa conference call to your knowledge; right?

A. To my knowledge, there is not.

Q. Did Mr. Oltmann tell you anything more about how he was able to get on this call in the first place?

A. I believe in his Conservative Daily podcast, he enumerated how he came on to this call.

He shared with us the reason why he was on this

call, and the reason given was he was -- he was investigating local, as in Colorado -- local journalists who were affiliated with Antifa.

These journalists, he suspected, were the journalists who were attacking his organization, FEC United. And this, to us, was reasonable as to why he was on this call.

As far as the Antifa call itself, this -- around this time, we were also -- I was reporting personally on stories where groups like Antifa, such as the Sunrise Movement, for instance, were convening on conference calls and colluding on ways to act upon their rage against Donald Trump and create chaos during the election season.

So all of this came -- combined contextually gave us a lot of reason to believe that Joe Oltmann was on this call for the reasons he stated.

MR. CAIN: Objection. Nonresponsive.

Q. (By Mr. Cain) I'll try to break it down into little pieces.

Did Mr. Oltmann share with you how he was able to get on the call, just from a functional standpoint?

A. I believe he stated that he was on a phone -- like, a phone call. It wasn't a Zoom call or a Skype call, as far as I understand, but it was a telephone call.

I don't recall him telling me exactly. I remember seeing his reports -- or his own statement saying that he had been working on this for a long time, and he had been listening in on these calls for quite some time before he came upon this statement about Eric Coomer.

Q. Okay. And for purposes of these questions that I'm going to ask you right now, I want to limit it to not what -- what's publically available, for example, on the Conservative Daily podcast. I just want to talk about your interaction with him as part of this piece. Okay?

A. Okay.

Q. All right. So did he tell you when this call occurred, like a specific date?

A. I don't -- I don't recall. I think he said -- I think he said sometime in October.

Q. Did he -- did he identify for you, aside from himself and, allegedly, Dr. Coomer, who else was on the call specifically? Not numbers, but identity of individuals?

A. I don't recall discussing other names on the call. My interest was in his story about Eric Coomer.

Q. Did you ask him to identify any other potential witnesses to the statement that was made, allegedly, by Dr. Coomer on this call?

A. I don't think so. My -- again, my focus was on

the statement made by Eric Coomer and what Joe Oltmann had heard on this call. So I only wanted to focus on the -- on this portion of Mr. Oltmann's story.

Q. On -- I'm sorry. Which portion are you referring to?

A. The portion where he's talking about Eric Coomer.

Q. Okay. Well, I'm asking about the statement here on the exhibit we're looking at.

My question was, did you ask him to identify any other witnesses that you could confirm, you know, that Dr. Coomer was actually on this call and made the statement?

A. No. That was not relevant to me.

What was relevant to me was the statement that Oltmann was telling us that Eric Coomer had made on this call.

What was relevant was then confirming Eric Coomer's identity, his background, his role at Dominion; in fact, if he was, in fact, working on Dominion, and then his own Facebook postings showing his radicalism.

Q. But you had -- you had one source available to you, in the form of Mr. Oltmann, to confirm that Dr. Coomer actually made this statement; right?

A. Correct.

Q. And it's -- it's fair to say that if you -- if you wanted to fact-check that or verify it, that you had the potential to talk to other witnesses to confirm this story. But you didn't --

A. There's always -- yes, sir. Sorry.

Q. Okay. But you didn't -- you didn't do that?

A. There's always potential to talk to any number of witnesses in any given element of a story.

Again, this -- the notes that Joe Oltmann had made about this call, this is not focus of our story about Eric Coomer. Our focus of the story was verified in the fact that we were looking at Dr. Coomer's role, title, and his own statements. So that was the part of the story that we were verifying.

Q. Well, so you weren't verifying other parts of the story that wasn't the focus in your mind?

A. In my mind, this statement from Dr. Coomer quoted -- attribute -- that Joe Oltmann had shared with us was relevant, in that this was the statement that caused us to look at Eric Coomer to begin with.

Without that statement, without the interview with Michelle Malkin, we never knew about Dr. Coomer. So that statement --

Q. That statement --

A. Correct.
(Simultaneous speakers.)
Q. I apologize. I just wanted to make sure that I understood when you say "this statement," you're referring to the one on the screen?
A. Yes. I'm sorry. I didn't clarify.
Yes. The statement "Trump won't win. I made F-ing [sic] sure of that," was the phrase that was associated with Eric Coomer, was causing Eric Coomer to be, hashtag, #trending, on Twitter for several days, I believe. And that was the entire reason we even knew of Eric Coomer.
So it's relevant to show the spark that created the blaze that ultimately is Dr. Coomer's own story, the facts that are indisputable about him.
Q. This being one of them, that he said this -- indisputable?
A. This -- yeah. This statement is coming from a witness: Joe Oltmann. And any viewer can look at Joe Oltmann and decide for themselves whether or not they believe Joe Oltmann is telling the truth or not.
We believed Joe Oltmann is telling the truth, in that he was on Antifa call; that he heard Eric from Dominion make the statement "Trump won't win." We believe -- we have no reason not to believe Joe Oltmann in

this case.
But this -- not an indisputable fact. The indisputable facts that we moved forward as a news network and put in "Dominion-izing the Vote" was the fact that you have an individual who is in a very high-level position at a company that dominates one-third of the U.S. election system, with very partisan, radically partisan, sentiments, and evidence that he was acting on those sentiments. That was the portion that was newsworthy, and that is undisputable.
MR. CAIN: Objection. Nonresponsive.
Q. (By Mr. Cain) Let's -- I want to talk about nuts and bolts, not -- not the determination of relevance, because that's ultimately going to be someone else's job here.
Just as far as this call goes, that's the focus of what I'm asking about. Obviously, you weren't on the call, so you don't have any firsthand knowledge; correct?
A. Correct.
Q. Your only witness to the call is Mr. Oltmann; correct?
A. Correct.
Q. Mr. Oltmann disclosed to you that he made notes of the call, did he not?
A. Yes.

Q. Mr. Oltmann was never asked by you or your organization for copies of those notes; correct?
A. Mr. Cain, with respect --
Q. Just answer my -- did you ask him for the notes or not?
A. His notes were about as relevant to me in this story as, say, Mike Tyson's bodyguard. It really was not the focus of the story regarding Eric Coomer. It was the spark that caused us to look deeper into Eric Coomer. And that's my answer.
Q. So did you ask for the notes or not?
A. I did not ask for the notes. I did not need the notes.
Dr. Coomer spoke to me, he spoke to you, he spoke to his friends and family through his Facebook postings that we were looking at, provided to us by Joe Oltmann -- 80 screenshots of Dr. Coomer's own words.
Q. Okay. Well, the statement that's on the screen is attributing the potential than Dr. Coomer was rigging the election and boasting about that. That's a fair interpretation of that statement, isn't it?
A. That is a fair interpretation of that statement.
Q. So don't you think that would be important to Dr. Coomer to be quoted as such in national media?
A. Important to him, how so?

Q. Well, he's been accused of a crime here. He's being quoted as saying he rigged the election; he made sure of it.
So to be fair to Dr. Coomer --
(Simultaneous speakers.)
A. -- he was rigging the election.
MR. RHODES: That -- that -- I was about to object to the question, but Ms. Rion has taken care of it herself.
THE REPORTER: I didn't hear the answer.
A. I'm sorry. I don't believe Dr. Coomer said he was rigging the election.
Q. (By Mr. Cain) Well --
A. We don't -- we don't have evidence that Eric Coomer said -- stated that he rigged the election.
Q. All right. You and I can agree to disagree.
The point of my -- my questions is to find out exactly -- it may not be relevant to you, as you've testified, but it's relevant to Dr. Coomer.
You didn't have -- did you ask Mr. Oltmann for anything to verify, beyond what we've discussed, that this call actually ever happened?
A. I asked if there was a recording of this conversation, and Joe Oltmann provided me with an answer, to me, that was reasonable.

His answer, I believe, was that he was -- he was -- this was a long-form series of calls that he was listening into. He never really expected anything newsworthy or notable to come out of these calls, so he didn't sit down and record hours of phone calls that he was on; rather, he was simply trying to identify who was on the calls.

It was for the purpose of identifying the journalists who were activists affiliated with Antifa attacking his organization, FEC United.

This is the story he told me, and I found that to be a reasonable explanation as to why there was no recording of this particular statement.

Q. Had -- had you used Mr. Oltmann as a source for any of your reporting prior to this piece?

A. I don't believe so.

Q. And you stated a couple of times that you thought he was credible. Can you tell me what about Mr. Oltmann you thought was credible?

A. Well, there are two parts to that -- two parts to my answer.

So, number one, you're looking at the credibility of Mr. Oltmann's -- how he's representing himself. He represents himself as a -- an entrepreneur, the owner of a data company.

He represents himself as a political activist, a conservative, who was actively seeking to expose Antifa in the state of Colorado.

Those parts we were able to verify by looking at his own data website. He had a website -- a company called PIN Networks, and it has over -- over 50 employees. He is clearly the CEO. So he was representing himself correctly there.

He was affiliated with FECUnited.org. We looked at his website. Indeed, he is an activist. We saw an October 16 article from Colorado Political or Political Colorado. I forget what the exact title of that article was.

But it's dated October 16, where Joe Oltmann is cited as being an activist against Antifa, trying to expose radical leftists who were creating -- causing havoc in his state and against him and his group.

We listened to his podcast, his Conservative Daily podcast, confirmed that he was, indeed, a conservative, and he was an activist.

As far as the motives -- that's the second part. The second part of verifying his credentials, kind of, viewing him as a credible witness, was looking at his motives.

He wasn't -- he stated to us, and we found it

reasonable, that he was not on this call seeking to destroy Dominion Voting Systems, or he was not on this call this -- Antifa call -- to expose Eric Coomer.

He encountered Eric Coomer of Dominion by accident. And that accident was confirmed by the fact that he was listening in to these calls for a long period of time.

Eric -- Joe -- Joe Oltmann was -- his stated reasons for being on these calls was that he was trying to get to the bottom of which journalists in Colorado were affiliated with Antifa and actively attacking his group, FEC United.

Those -- that explanation that Joe Oltmann gave to us established for us his motives, and his motives, to us, were reasonable.

Q. What about his status as a -- as you put it, a conservative activist increased the credibility of Mr. Oltmann in your eyes?

A. It increased the credibility in that he was trying to expose Antifa, a radical leftist organization or a group-of-people movement. He was radically against Antifa.

And this was stated in news articles that we had found, as I mentioned just now. That, for us, affirmed his credibility in that realm.

Q. Thank you, ma'am.

In terms of his credibility, are you in a position to gauge Mr. Oltmann's credibility with that of Dr. Coomer?

A. How -- how so?

Q. Well, if he's a credible source to you as a conservative activist, is Dr. Coomer a credible source of information for this story to you as a -- in your mind, a left -- left-leaning activist or Antifa member?

A. As far as his own words, yes. He had Facebook postings showing Antifa sympathies. So, yes, in that regard, he is a very credible witness against himself.

Q. And how about when you reached out to Dr. Coomer? Were you able to get a comment from him to either verify he was on this call or not?

A. I was unable to procure a comment from Dr. Coomer. Charles Herring called me about a day after the Michelle Malkin interview, right in the middle of my working on "Dominion-izing the Vote," and asked me if I could get a hold of Dr. Coomer.

So I tried to find way to contact Dr. Coomer, and I did not succeed in that. As -- as -- as I would later experience and confirm, he became a ghost. He seemed to have scrubbed his profile online.

Q. How long did you try to contact him? And

describe your efforts in detail.
A. I don't remember the span of time, but I remember putting an effort into finding him.
I remember looking on all the social media platforms. I remember looking for his -- trying to find out what his middle initials were to find out if there was a way to find him on other sources.
I don't remember all the ways, but I remember I put an effort, because it was a request from my boss, Charles Herring, to go find this guy. So I put in the effort. I just don't remember all of the methods that I did to try and find him. But he was -- I could not find him, at the end of the day.
Q. Did you task anyone else in your -- on your team to try to locate Dr. Coomer for a comment?
A. I don't recall that I did. I may have. I don't remember.
Q. Did you send any communications to Dominion asking that they make Dr. Coomer available for this story?
A. I did not.
MR. CAIN: Rebecca, are you asleep yet, or are you paying attention?
MS. DOMINGUEZ: I am paying attention.
MR. CAIN: I know you are. Let's mark Item 11 in my folder. That relates to Watkins.

Q. (By Mr. Cain) So let's -- let's talk about -- we talked about, briefly, your outreach to Dr. Coomer and to Dominion.
We've talked about your outreach to Ron Watkins. I'll turn to that in just a minute.
And I forget -- forgive me. I'm having a senior moment. Did we talk about whether you actually sent a message or an outreach to any of the election experts that I showed you on the screen from that letter we looked at this morning?
A. I don't believe we discussed that, no.
Q. Okay.
A. Do you want me to answer -- I'll answer the question.
Q. I'd like to facilitate it as easy as possible. What I'll do -- maybe this will be the fairest way. Let me put this back.
Okay. You remember this when we were talking about it earlier?
A. Yes.
Q. Okay. And it's -- we talked about Professor Blaze and Professor Halderman. In connection with the "Dominion-izing the Vote" story, specifically did you reach out to any election experts outside of, potentially, Mr. Watkins?

A. I used the statements from Professor Halderman, and I included that in my special. But I don't recall reaching out to the individuals -- I can't see all of the individuals on this list, so I can't answer with certainty.
But I -- I don't -- I don't recall reaching out to Professor Halderman, that's what I can say for -- for sure. Because I was using his own report or his own statements from the New York Times opinion piece.
Q. Okay. Well, let's --
A. This is a long list.
Q. It is a long list. But you seem like a very bright and capable individual. Why don't you scan this list and just tell me if you -- outside of using, you know, some clips from Mr. Halderman in the prior piece, I'm asking you whether you specifically attempted to contact any of the -- the individuals on this letter.
A. I don't remember. I --
Q. I'll just, kind of, scroll down through it. There we are.
As you sit here, can you think of any -- anyone, either on this list or off this list, that was an election expert that you contacted for this piece?
A. I can only identify Dr. -- Professor Halderman and using his -- his report or his statement in the

New York Times opinion piece.
Q. Okay. Thank you.
I'm going to show you what I've -- well, Rebecca technically marked as Plaintiffs Exhibit 59. And this is -- this is the person you did contact and interviewed about this piece, Mr. Watkins; right?
A. Yes, sir.
Q. Earlier you told me he was or is a systems penetration tester. And here, he's referenced as a large-systems technical analyst.
So let's talk a little bit about Mr. Watkins. Did you know him before you interviewed him for this piece?
A. I did not.
Q. Do you know -- well, let me ask it a different way. How is it that you first came into contact with him?
A. I first saw Mr. Watkins' Twitter profile commenting heavily on the Dominion Voting Systems user manual. And he seemed to be dissecting the manual analytically in a way that I did not see anybody else dissecting at the time.
His analysis was detailed and seems to be very thorough. So it naturally sparked my interest. This was related to the story I was working on, you know, election vulnerabilities in other machine systems.

And he was on Twitter. I contacted him on Twitter, I think, and from there, asked him if he was willing to interview with me about his analysis.

He agreed to an interview. I spoke with him on the phone, again, just to, kind of, verify he was Ron Watkins and he was the guy I thought he was -- he was on his Twitter profile. And then we sat down for a Skype interview.

Q. Okay. So let's -- let's break that down a little bit.

The two descriptions that I said -- well, you said -- systems penetration tester and large-systems technical analyst -- where did those descriptors come from?

A. Those are descriptors Ron Watkins gave of himself, which seemed consistent.

I asked -- I asked him of his background, and he said he was a large-systems data analyst. I think -- I guess the titles can be changed, a large-systems technical analyst, I think they're about -- they describe the same role.

And he said -- Mr. Watkins told me that he studied this in grad school, and he was someone who did this for a living.

Q. Okay. So let's -- do you know as you sit here

what a large-systems technical analyst actually is or does?

A. The way that I understand it as I sit here now, Mr. Cain, is that a large-systems data analyst or technical analyst looks at a system and then analyzes the patterns and vulnerabilities within that system.

So it's kind of self-explanatory, in that a large-systems analyst -- he'll look at the vulnerabilities and the patterns that can be identified within that system.

He stated that he was a penetration tester, which, I think, in layman's terms, is kind of a hacker or a white-hat hacker. I don't know what the different hats are.

But from looking at his own verifiable background, I could see that he was an administrator for 8chan, which is an anonymous messaging board, I guess. And the platform 8chan is famed for being able to be an anonymous, I believe.

And so that, to me, spoke to the technical credibility of Mr. Watkins in the sense that, a lot of times, these guys don't have traditional resumes, if you will. They often have profiles that are maybe nonexistent online. They make it a business of not being known online. Or if they are known, then the product -- their

product should speak to their expertise.

And in this case, Mr. Watkins' product that I could verify seemed to be that he was an administrator with 8chan, which, in his own words, I think he resigned from that post at some point in 2020. But that was verifiable to me.

Q. Do you know what an administrator does on a site like 8chan?

A. I don't think I can speak with confidence. But I know that he was involved in making -- for example, building a crypto currency for 8chan users.

I think that -- it implied that he was someone who controlled or at least ran that platform and had the technical expertise to maneuver throughout it by designing a crypto currency, for example.

Q. Was 8chan -- if you know, was that where the QAnon postings were happening at one point?

A. I don't know. I really -- I've never ever been on an 8chan board, so I wouldn't know.

All I know is the reputation of 8chan as being an anonymous messaging site or, at least, website, something like that.

Q. And I -- and forgive me. I didn't understand the significance of that.

What about it being an anonymous testing site

made it -- or website made Mr. Watkins seem credible to you?

A. It seems like it would take quite a bit of technical expertise to be able to build or administer a site like that.

Q. Because you don't -- you honestly -- if you're administering the site, do you know whether he actually built the site himself?

A. I -- I believe he had a role in building it. But I cannot tell -- I -- I don't deign to understand fully his entire role in 8chan. I just know that he was deeply involved in its creation and maintenance.

Q. And did you -- did you find out any information as to -- as to what type of clients Mr. Watkins had served historically when he was engaged in large-system technical analysis?

A. I wouldn't -- I did not know that. I do not know that.

Q. Do you know how long he served as this type of analyst just in terms of his work experience?

A. Again, I think a gentleman with this kind of profile does not have a traditional CV or a traditional resume, so I wouldn't know that, no.

Q. You mentioned something about grad school. What did he describe to you, if anything, about his educational

background?
A. He mentioned grad school in passing. And I believe it's in our interview, actually, where he talks about how he studied -- or he was a penetration tester, which, again, is -- in layman's terms, is basically a hacker, and that he did that all through grad school.
So I don't --
(Simultaneous speakers.)
Q. I'm sorry.
A. -- details about it.
Q. I apologize.
My question was going to be, what, if anything, did you do to look into his -- his educational background?
A. I didn't dive too deeply into his educational background. I spoke with him at length to confirm that he was, in fact, the individual who was analyzing the Dominion voting user manuals. And to me, that was what was relevant.
The relevant -- the credibility -- when you're identifying the credibility of an individual of this nature, there's a different set of credibility, I guess, prongs that you're considering. And in this case, it's the product. What is this guy's product?
His product was his analysis of Dominion Voting Systems' user manual. He was one of the

few, if only, individuals that I knew of at the time conducting such in-depth analysis of Dominion's voting machine manual and user manual.
So to me, that was what was more relevant than checking his exact degree at whatever university he went to.
Q. Okay. So but my question, nonetheless, remains, do you know where he went to school and what degree he has?
A. I do not know where he went to school.
MR. CAIN: Rebecca, can you mark as the next exhibit Item No. 3 in my private folder?
MS. DOMINGUEZ: Yes, sir.
Q. (By Mr. Cain) You said you reached out to Mr. Watkins on Twitter. Were you following him at that time?
A. I was not.
Q. So how did you -- do you remember how it is that you directed yourself to his Twitter page?
A. I believe so. I was -- I mean, I was researching election-system vulnerabilities. So I'm constantly trolling Twitter and constantly trolling a variety of sources. And I came across his very lengthy threads and analysis using screenshots of the Dominion Voting Systems manual and breaking it down and

discussing what they meant and what they -- what he was finding.
So it was in the process of generally researching for "Dominion-izing the Vote."
Q. Now, Mr. Watkins is banned from Twitter now, is he not?
A. He is. I believe so.
Q. I'm going to show you what I'm marking -- again, Rebecca marked, as the next exhibit.
(Plaintiff's Exhibit Number 60 was introduced.)
Q. (By Mr. Cain) This is Exhibit 60. And I'll blow it up and make it, hopefully, a little easier.
Okay. So do you recognize Ron @CodeMonkeyZ? Is this the same individual we've been talking about?
A. Yes, sir.
Q. Okay. And does this look like the Twitter page that you went to when you were looking at possibly interviewing Mr. Watkins for this piece?
A. It does. Yes, sir.
Q. Actually, up here it says -- this is November 3rd: "I'm resigning as admin of 8kun effective immediately." And then he goes on to talk about that.
You talked about 8chan. Do you know what 8kun is?
A. I believe -- I believe they're the same thing.

I don't know why they're spelled differently. Again, I'm not a user of 8kun or 8chan. But I believe they are essen- -- are the same board.
Q. Okay. So let's -- let's go back in time.
You're looking at his Twitter, and you're seeing him posting about election security interests, or issues, and that's what caused you to refer out; fair?
A. Yes. Fair.
Q. And he even references here on this page, "Ms. Chanel Rion just reached out to me, and I'll be talking with her about Dominion tomorrow." Do you see that?
A. Yes, he does.
Q. So about how much time did you spend with Mr. Watkins on this -- this reach-out that he's referencing here, if you remember?
A. I recall about -- the actual interview was about an hour or 70 minutes. And then I spoke with him before the actual recorded interview. I don't remember how long I spoke to him before that, but at least an hour ten, 20 minutes in the actual interview that was recorded.
Q. And I think you've -- you've said this, so we don't need to go over it. But, essentially, you were piqued -- your interest was piqued by the fact that he was -- he was in a position to analyze the system through

reference to the user manuals that Dominion had; is that fair?
A. Yes, that's fair.
Q. He indicates here that he reached out to Rudy Giuliani, as well, about this topic.
Did you -- at this time, were you in contact with Mr. Giuliani about your reporting on this topic?
A. I interviewed Rudy -- Mr. Giuliani for the special, and I did not discuss -- I never discussed Eric Coomer or anything like that with him. I was discussing general election vulnerabilities with Mr. Giuliani.
And when I say "discuss," Mr. Cain, I meant I was interviewing him and including that in my special.
Q. I understand.
Were you -- through this period of time and up to the point where this -- this piece went -- was broadcast, were you in contact with anybody from the Trump administration or their campaign about the work that you were doing on election rigging stories?
A. I was in contact with all of these -- Rudy and Sidney Powell and Trump campaign, because I was interview -- or I was interested in interviewing them. So, naturally, I would -- I have a back-and-forth communiques with all of these groups that you mentioned.

Q. Who was your point of contact at the Trump campaign when you wanted to go out and see if you could get an interview on a particular topic like this?
A. Oh, there were different individuals that I would contact at any given time. Oftentimes, I would just directly contact the individual I was trying to interview.
So, say, if I'm trying to reach out to Jenna Ellis or Eric Trump on Don Jr., I would contact them directly, usually.
Q. You had their -- their personal contact information?
A. Their campaign information, yes.
Q. Well, if you wanted to call, let's say, Eric Trump, right now, would you have the ability to do it? You have his cell phone number, that sort of thing?
A. Yes. I believe that's his cell phone number.
Q. All right.
And so my question, to loop back, do you recall if you contacted -- you've talked -- other than what you described -- individuals that you described -- do you recall contacting anyone with the Trump campaign about the reporting you were doing in this piece?
A. I do not recall that.
Q. Do you recall if you asked a campaign spokesperson to give a comment on it or not?

A. I may have. I don't remember, but I may have. It would not have been unusual for me to reach out to the Trump campaign for comment on a story, but I don't remember that in this particular piece.
Q. Who did you understand to be -- and it may be multiple parties -- who was acting as a spokesperson for the Trump campaign in November of 2020 when you were doing this piece?
A. Oh. I don't -- that's a difficult question, because there were different, I guess, spokespeople for different portions of the Trump campaign. So do you have a particular area?
Q. Well, I mean, I don't know who you would -- for something like that this -- we're post election and there's -- as you know, President Trump had been alleging voter-fraud-related issues for months.
So who would have been at the campaign that you would have talked to about, you know, potentially giving information or an interview for this type of story?
A. I believe it would have been -- if we're talking about election vulnerabilities, I think it would have been Rudy Giuliani at the time.
But again, these roles were switching all the time, so I was -- I was talking to any number of people on the campaign for different stories that I was working on

at any given time.
But to answer your question, in this particular context, I believe Rudy Giuliani would have been kind of the -- the voice for -- for the Trump campaign in terms of discussing election vulnerabilities, or at least he was viewed as that -- as taking on that role at the time.
Q. And that's how you viewed it yourself; right?
A. That's how I viewed it; although, there were other spokespeople, too, involved in the Trump campaign, and they were also in flux. But I don't remember all of them.
Q. How about Ms. Powell? Did you view her as a spokesperson for the campaign?
A. No. I don't think I viewed her as a spokesperson for the campaign.
Q. And tell me why? Because, obviously, you saw the press conference they did on the 9th. It would have been a couple of days before your reporting, and Ms. Powell was there.
Why -- why is it that you didn't view her as a spokesperson or representative of the campaign?
A. I understood at that time that she wasn't paid by the campaign. So if you're not paid by an entity, then I don't think you have a formal relationship with them.
She may have been helping provide research, may

have been working closely with the campaign. I understood that. But I did not understand her to have a formal contract with the campaign.

Q. But you did -- you did understand that as it relates to Mr. Giuliani?

A. I don't know if I can answer that. I believe so. I'm not sure.

Q. Well, that's why I'm asking --

(Simultaneous speakers.)

A. I can clarify, Mr. Cain.

I guess, just in the -- in the day-to-day operations in this world, I mean, Mr. Giuliani had known Mr. Trump for decades, and now President Trump -- then President Trump for years. They were very close.

I did not have the understanding that then President Trump was close to Sidney Powell. So I guess I merged -- I did not really ask Mr. Giuliani if he had a formal contract with the Trump campaign. I assumed that he did.

But I knew that Sidney Powell did not have a formal contract with the Trump campaign, if that makes sense. Hopefully that answers your question.

Q. I'll resist commentary.

You made the distinction about monetary compensation being a factor for you. That's why I asked

you about Mr. Giuliani, because there's been some reporting about payment, or lack thereof, with him.

But as it just relates to Ms. Powell, the basis of your statement previously that you didn't consider her to be a representative of the Trump campaign is -- is tied to the lack of compensation. Is that a fair statement?

A. I believe so. Because I've -- I believe -- I believe Sidney Powell was stating this in her own words, wasn't -- again, I cannot -- don't want to say on record something that is false.

But I believe Sidney Powell was saying this in her own words; that was she wasn't working for the Trump campaign; that she was simply helping them in their research and in their legal research.

Q. Well, fortunate for us, the campaign is going to be deposed here shortly, so they can clarify it.

Let's get to -- since our time is dwindling --

MR. CAIN: And by the way, Mr. Videographer, I do want a ten-minute warning before our three hours is up just so I can collect my thoughts.

THE VIDEOGRAPHER: Yes, sir.

Q. (By Mr. Cain) So I assume that you read through the statements that Mr. Watkins made before you interviewed him about the Dominion software? That's why you decided to interview him, essentially?

A. Yes, sir. I can't say that I've read through every single statement he's made, but I remember reading enough to where I determined I would like to talk to him.

Q. Do you remember reading this comment that's, kind of, in the middle of the page where he says, "The software seems to be legitimate" [sic] -- or, excuse me -- "legit and well written."

"It passes independent security audits and probably works as intended. The issue is the amount of control the software gives to the local IT guy, who can ultimately decide the fate of a nation."

A. Yes, sir. I remember reading that statement.

That statement was particularly intriguing to me. And one of the reasons contacted Mr. Watkins was for him to explain in detail why he made the statement.

Q. Okay. Did you -- I know we've talked about this, kind of, at length. Have we -- have we described just, kind of, in your mind's eye, all of the reasons why you -- you thought Mr. Watkins should be the person that you interviewed for this piece; the status as a large-system technical analyst, and then the work he was doing as reflected in this exhibit?

A. Yes. I believe we discussed that. And my answer, if I recall correctly, was that he was one of the few people commenting in detail about the -- about

Dominion voting, you know, software, the software side of, I guess, these voting systems.

And he was one of the few individuals that I knew of who he was looking into the use everybody manual. He ultimately provided us -- provided me with about a thousand -- about a thousand pages worth of documents, including the two user manuals, user guides, from Dominion and various publically available documents on secretary of states' websites and others.

Q. You being in Washington, I'm sure -- well doesn't -- not because you're in Washington, D.C., but surely you've followed the QAnon movement. Hard to miss it.

A. I know of it.

Q. And --

A. I don't know that I follow it, but I know of the QAnon movement.

Q. Okay. And that what's your understanding, if you have any as you sit here, about Mr. Watkins' association, if any, with QAnon?

A. I really don't know. I know that he has been speculated as being affiliated with QAnon, but I don't know that at all.

Q. If it turns out that he is a -- well, let me just back up.

Do you view QAnon -- my understanding, which is limited, is that there's something called a "Q drop," where this person will post anonymously on the same form that we've been talking about, 8chan and/or 8kun.

Is that -- does that ring a bell to you? Did you know that before I just --

A. I really don't know what forum QAnon actually operated on. I know that when a, quote, "Q drop" would be dropped, I guess, oftentimes, they were just reshared on social media. So I -- I don't know what form they exclusively posted on.

Q. Okay. Well, I'm trying to -- let me drill down a little on this and what you knew about Mr. Watkins.

And you told me you know he was administrator for 8chan; right?

A. Yes, because he stated on his own -- in his own words that he was resigning from 8kun, or 8chan, as administrator. So that, to me, confirmed that he was, in fact, involved in 8kun/8chan.

Q. Okay. Did you know as -- as part of your research on Mr. Watkins that 8chan and 8kun has been criticized because of its -- because of this anonymous posting?

It has hosted -- the site has hosted things such as the mass shooter manifestos. It's been criticized for

hosting child pornography and racist memes. Did you know anything about that as it relates to 8chan or 8kun?

A. I knew that it was a controversial site. I don't remember why. But I know that it was controversial, in that it was anonymously hosted, I guess. And that's about the extent that I understood the site.

I also understood that you don't -- a website does not necessarily take -- or a forum like Google does not often take responsibility for everything it hosts.

So even if there were questionable elements about 8chan or 8kun, I did not think that was degrading to Mr. Watkins' analysis of Dominion Voting Systems.

Q. Well, do you know what an administrator actually does for a website such as 8chan?

MR. RHODES: Objection. Asked and answered.

Q. (By Mr. Cain) And by this, I'm directing it more -- since your counsel made that objection -- to the ability to control content.

A. Right.

I -- I don't know to -- I don't know how 8chan works. I don't know how it operates. I don't know what the extent of administrator -- how much control they have on a website like that.

I only knew that he had a big role in its existence as a general free-speech platform, and that was

sufficient for me to move forward and talk to him.

Q. Have you happened to watch -- I think HBO did a series, a six-part series on QAnon. Did you -- did you happen to catch that?

A. I know of the series. I never sat down and watched to whole thing. I think I've seen bits and pieces of it.

Q. Did you see the part where, you know, the conclusion that was drawn was that Mr. Watkins was either QAnon or, perhaps, his father was or they collectively were?

A. I knew of that speculation.

Q. As you sit here today, are you concerned that the source you used for "Dominion-izing the Vote" -- sorry. We've got a kid screaming.

Let me -- let me --

A. Not Atlas.

Q. That is not Atlas.

I'll ask it a different way. Based on what you know about Mr. Watkins today, as you sit here, do you still believe that he's a credible source for your reporting on "Dominion-izing the Vote"? And if so, why?

A. Yes. To the extent that he commented in "Dominion-izing the Vote," I believe the analysis he provided to us was sound and stands to this day.

Q. And given the second part of my question, why is it that you still hold that belief today?

A. You can -- if you watch the piece, you'll see his analysis, and it matches -- his analysis matches with what he is analyzing in the user guides and just -- it -- it all checks out.

Q. Well, his analysis -- we don't have time to look at that -- that part of it -- was that some -- some of the two to six individuals involved in the adjudication process could change votes in a manner that didn't reflect voter intent. Is that a fair summary of what he said?

A. I believe so.

Q. He didn't say that actually it occurred, to his knowledge, during the election; right?

A. He was very clear on that. In fact, he -- he was very clear to say that he -- he had never seen or actually held or touched a Dominion voting machine; not to say that other hackers haven't. We know that these machines are available for purchase on eBay, and you could hack them, as we saw in these hackathons.

Mr. Watkins was very clear that he was only drawing his conclusions based on what he knew as a penetration tester. He's reading these user guides as a penetration tester. And he made very clear that his analysis was based on these user manuals that he was

referencing -- the two that he shared with us -- in addition to the certification documents provided through the states of Pennsylvania and -- what else -- Texas, other states.

Q. But at the end of the day, it's fair to say that he is speculating about the ability to do that. He doesn't have any hard evidence that someone actually did so; is that true?

A. That's true.

Q. Let me ask you a couple of questions about -- turn the page -- about -- about issues of privacy.

And remember earlier, I asked about whether there were any formalized journalistic standards at OAN and ethical standards.

In your piece, you published a photograph and video of Dr. Coomer; right?

A. Yes, I believe so.

Q. In your piece, you -- you put quotes attributable to him about statements made on this Antifa call; correct?

A. Correct.

Q. And then you followed that up with information from a Facebook page that Mr. Oltmann had provided to you; right?

A. About 80 screenshots of Facebook postings by

Dr. Coomer.

Q. And as you -- you didn't know about Dr. Coomer before you started doing your research for this piece; right?

A. No, sir. I was made aware of Dr. Coomer's existence on, I'd say, November 13 or 14, shortly after Michelle Malkin's interview of him.

Q. But as far as you were aware, he was --

A. Sorry. Interview of Joe Oltmann. I'm sorry. I misspoke.

Q. Yeah.

But as far as you know, Dr. Coomer was a private individual working for a private election security company at that point, when you first got into this?

A. When I first got into this, I didn't know anything about Dr. Coomer.

The -- how I familiarized myself with him was his public patents that were posted. And he appeared to be in promotional videos and -- for Dominion Voting Systems, and he was representing Dominion in news articles.

He was -- he seemed to be a pretty public face for Dominion Voting Systems at the time.

Q. But in this -- in this context, I guess, Mr. Oltmann told you he had -- he was able to get a hold

of private Facebook pages for Dr. Coomer. That's what he told you; right?

A. Yes.

Q. And the only thing he told you about how he got access to that is he did so, quote, "legally," closed quote; right?

A. Yes.

Q. But he didn't tell you anything specific about how he was able to get access to this -- to this private page?

A. No specifics.

Q. Okay. And you didn't ask?

A. No. I just -- he said he ran a data company, and he was able to access these private pages.

Q. Did you weigh -- in thinking about putting this piece together and broadcasting it, did you weigh the consequences of publishing personal information of Dr. Coomer, as you understood it? Did you give any weight to that?

A. Did we -- I don't believe we published -- are you saying -- Mr. Cain, are you saying that we published personal information about Dr. Coomer?

Q. Yeah. I'm saying -- and I don't mean that in the form of a driver's license number or a social security number.

What I'm saying is, did you give weight to the fact that you were publishing personal information, i.e., personal posts on a private Facebook page, prior to doing so in this report?

A. At the time we published this report, the posts of Dominion were already in the public sphere. They were already being reported on and discussed by other news outlets and by, I guess -- I mean, he was trending on social media, so people were sharing Dr. Coomer's postings already after Michelle Malkin's interview.

So we went about seven days after -- seven or eight days, I believe, after Michelle Malkin's interview of Joe Oltmann. Of course we consider the safety of -- you know, of anybody as we are putting out our stories.

But in this case, Dr. Coomer's story was out and discussed in the public sphere before OAN went to air with it.

Q. Well, OAN may have its own unique set of viewership beyond these other media, presumably.

So my question was, what consideration did you give, if any, to putting this type of information out on your broadcast? Did you weigh the consequence of doing that?

A. I mean, I myself -- I mean, if you're saying if I myself am sensitive to this, I -- I am. I know what it

is like to get death threats. And I know everyone says that.

But, you know, I've -- my husband ran for public office a couple years ago, and we were receiving death threats like, you know, I'm going to throw kerosene on your husband and tie him up and rape your wife while you watch.

I mean, we've received death threats like that, and I understand the weight of such death threats or such threats that come of taking a position or taking a stand.

Dr. Coomer took several stands and several positions, in his own words, and posted them within his -- his sphere, his friends and family and his Facebook postings.

And I think you have to take responsibility for the positions that you take. And I think that's -- that's something that Dr. Coomer should be taking responsibility for as well.

The story was out long before OAN published on November 21st.

Q. What -- how are you drawing, just in your own mind as you're reporting on this topic, the link between someone being against the President Trump, whether it's policies or otherwise, and then their ability to do their job professionally and without trying to rig the election?

Do you see what I'm saying? How are you linking those two things?

A. How am I linking words with action?

Q. Yeah.

So earlier you -- you said that Mr. Oltmann was credible as a conservative activist, and that was part of what you relied on.

If we assume Dr. Coomer doesn't like President Trump, I'm having a hard time with the link that you're drawing between that and actually committing a crime.

A. Well, if you look at Dr. Coomer's Facebook postings, he calls on his friends and his family to take action against Trump; in this case, unfriend him or don't associate with him in any way, shape, or form if you are a supporter of one political party.

He seemed to carry a lot of rage and carry that through in telling his followers and his friends and family to act on his rage. I think that -- that's a reasonable link.

Q. Well, okay. How about if you combine that -- the element that we've been talking about previously with the statements he's allegedly made in this Antifa call?

At the end of day, that was a material part of you drawing the link between the Facebook pages, his

status with the company, and actually having the ability to do what was suggested in your piece; right?

A. What's your -- and your question is?

Q. My question, to be more succinct, is do you still have a story, in your mind, without the Antifa conference call on Dr. Coomer?

A. Absolutely.

And I think I said this earlier. The newsworthy element of the Dr. Coomer part of this story is the fact that you have a very partisan actor who is radicalized. He has extremist views and seems to have extremely violent views of President Trump and those who follow President Trump or vote for him.

Combine that with the fact that he has -- his title at Dominion Voting Systems -- he's head of security and strategy and was formerly an engineer.

Ostensibly, he had access to a very important company who had a dominant share -- a dominating a share in the U.S. election systems.

So it's a newsworthy -- it's very newsworthy to us that someone with that extreme set of views held a very high-level position at a voting company; and that voting company holds about 30 percent of the United States election systems.

Q. And if he would have had conservative views of

that extremity, would you have similar concerns?

A. I think if he had conservative views, he would not be speaking in a courtroom, but he would be speaking in a -- in front of the FBI or the DOJ.

Q. Because he would have been prosecuted unfairly?

A. I believe so.

Q. Now, you had put -- let me do this.

MR. CAIN: Actually, where are we on the video? I may just want to take a break and get the last few segments lined up. Time?

THE VIDEOGRAPHER: There's 12 minutes remaining, sir.

MR. CAIN: Okay. Let's go off the record, and then we'll complete our 12 minutes here. I only need -- I only need about eight minutes, as you said earlier.

THE VIDEOGRAPHER: Going off the record. The time is 3:16.

(Recess from 3:16 p.m. until 3:25 p.m.)

THE VIDEOGRAPHER: Back on the record. The time is 3:25.

Q. (By Mr. Cain) Okay. We'll jump around for a few little topics, and then our time will be done.

Let me show you what I have -- I marked as an exhibit in Mr. Herring's deposition. He wasn't really able to inform me about some piece of this.

This is Exhibit 41. You remember when I was asking Mr. Herring about this text?
A. Yes.
Q. This was between you and him while you were in the White House press briefing room?
A. Yes, sir.
Q. And in terms of the White House, you made some news in some of the questions that you asked, including the question of President Trump about voting by mail as it relates to the pandemic. Do you remember that?
A. I think I asked daily questions. I don't remember exactly my question. But it sounds like I asked that question.
Q. Well, I -- the thrust of my question is coordination, your relationship with the Trump Administration campaign.
When you were asking questions of President Trump, were those questions being provided to him beforehand so that he understood what was going to be asked by OAN?
MR. RHODES: I'm objecting to this as, unless you're asking about Eric Coomer, completely unrelated to the topics in the -- relevant in this lawsuit.
MR. CAIN: Well, I think it goes to the relationship between these parties and coordination, and

this relates to voting issues. So I think it's a fair question, Mr. Rhodes.
MR. RHODES: I disagree.
MR. CAIN: Okay.
Q. (By Mr. Cain) Well, can you answer my question?
A. Sure.
The press office, any press office and, as far as I understand, most press offices in most administrations -- and this is from my conversations with my colleagues at the White House -- most press offices would ask news organizations for topics or general topics. And I believe Secretary Psaki, of the Biden White House, does this as well. She's continued this practice.
They -- the press office would ask news organizations for general topics for the day, just to figure out who they would call on and see if they could prepare a more detailed statement on given topics.
Occasionally I would be asked by the press shop at the White House, along with Bloomberg and New York Times, everyone who was sitting in the basement with me -- we would all be asked what topics we were working for the day, and whether or not the press office could prepare for it.
And I would often give my topics either verbally or through an email. It would usually be a one-line topic

saying, oh, I'm going to ask about Russia; if he can answer the question about, you know, Iran or whatever.
But I was not unique in that. They would -- the press shop would ask other news organizations for topics. And sometimes we would provide them, and sometimes they were just spontaneous.
Q. And that was your practice while you were there?
A. Not often. I did not -- I did not actually do that as much as the other networks did.
Q. Well, in this -- and this may or may not be related, but in the Plaintiff's Exhibit 41, what I was asking Mr. Herring about was this comment at the -- at the end -- not the "Can we countersue Coomer and get him in discovery," but "Big updates from tonight. No meeting, but it's for the better. Christina can fill in too. Adjustments had to be made."
Explain to me what you mean by that.
A. I don't remember. I -- I do remember this had nothing to do with "Dominion-izing the Vote" or Dr. Coomer or anyone -- any one of your clients. But I -- I honestly don't remember what this was about.
Q. The "big updates" doesn't strike any -- any bell for you as far as what you were talking about?
A. No. I mean, we could have been talking about the arrangement in our offices. I don't -- I don't

remember what this is about.
Q. I also asked Mr. Herring about this concept, internally or otherwise, at OAN about "H stories." Remember when I asked him about that?
A. Yes.
Q. And so I have the same question for you. Is that -- is that something -- a term that was used internally at OAN?
A. Not in the D.C. bureau, that I know of.
We -- we have a pretty tightknit group in our D.C. bureau, and we never used that term, at least when I was around.
Q. And I think you mentioned you've never even been to the San Diego office --
A. No, sir.
Q. -- right?
A. That's correct.
Q. And the way I -- the way it works is, once you complete your piece, it's then sent electronically to San Diego for the producers there to put on air?
A. Correct. I think they, like -- they do something with the sound, and they -- they review it just to make sure that the footage is correct.
And there's some general oversight that happens over there. I'm not familiar with the entire process.

MR. CAIN: Rebecca, I should have asked you this before. I think it's Exhibit 5, Number 5 in my private folder. Let me confirm that real quick.

MS. DOMINGUEZ: Would you like me to mark it?

MR. CAIN: Yes, ma'am. OAN 750 through 755.

Q. (By Mr. Cain) Earlier, Ms. Rion, you mentioned that you'd put up the Dominion website. I think it was when I was asking you: Did you reach out to anybody at Dominion? You remember that testimony?

A. Yes. Dominion Voting Systems' statement, I guess, addressing controversies involving Dominion voting at the time.

Q. Let me show you what's marked as Exhibit 61 to your deposition. Begins at OAN 750. What are we looking at here?

(Plaintiff's Exhibit Number 61 was introduced.)

A. This is the -- I think this is the screenshot that I used in my "Dominion-izing the Vote": Dominion Voting Systems' statement addressing controversy involving them at the time.

Q. (By Mr. Cain) Okay. So you can confirm for us that you had this information in your possession when you were preparing this report prior to broadcast?

A. Yes, sir.

Q. Okay. And I asked this of Ms. Malkin. There's

a reference to the joint statement by CISA and the department -- Department of Homeland Security on whether the -- the vote was compromised.

And to you I would ask do you consider both of those organizations to be authoritative as it relates to this topic?

A. As it relates to this topic, I know there are questions about CISA. I know that the head of CISA at the time, Mr. Krebs, was -- had anti rump sympathies, I believe.

And we also know that CISA had, I guess, on its -- there was some kind of affiliation where they brought in Dominion Voting Systems itself as one of the members of a committee that CISA hosted or had.

So there's some questions about CISA's credibility at this time when they made that statement.

Q. And credibility in your mind -- because I asked -- well, confirm this for me. I'll back up.

Mr. Herring identified OAN as a pro-Trump network. Would you agree with that characterization?

A. Sure. I would agree with the characterization, too, that we -- you know, as far as -- if you're asking about bias or what our leanings are, we don't hide the fact, or I don't hide the fact that I'm not a big fan of big tech or big government or extreme leftist activism.

So if that's the bias you're asking about, then there is mine; and I'm quite open about that.

Q. And you're open about your support of former President Trump too, openly?

A. As far as -- so long as he's against big tech and big government and all the things that I just listed to you, yes.

Q. So on this page, you're critical of Former Director Krebs because he's anti-Trump, I think, was your word.

What about the Department of Homeland Security? Do you consider them to have been authoritative as it relates to issues concerning election integrity?

A. I don't -- I don't want to answer that now, because I know that there were some questions, also, in -- in the way that they -- that certain officials within DHS conducted themselves during the Trump Administration.

And as far as Krebs's credibility, I want to qualify. It's not just that he was -- he seemed to be anti-Trump, but it was also that he had -- he also came back with a statement on his own Twitter account saying that he -- qualifying his statement, saying that he never said that there was no fraud at all. I'm paraphrasing, of course.

But he also seemed to, kind of, hedge his own

statement here: There is no evidence of voting system -- votes being lost. I think he qualified his own statement.

So there's -- there's a lot in the air when it comes to CISA's credibility at this time under Chris Krebs.

I believe he was also friends with Miles Tyler, or Miles Taylor the, alleged author of Anonymous, who was also pretty rabid anti-Trump figure.

There's just -- there's definitely some questions when it comes to CISA's credibility and impartiality here. And that's where I stand.

Q. Where you stand is you have some questions about the credibility of Mr. Krebs, but you cannot identify any questions, in your mind, concerning the credibility of Ron Watkins, who made it into your -- your report?

A. I -- as -- as it stands here today, I do not question the analysis that Mr. Watkins provided for us in "Dominion-izing the Vote." And I think that's the relevant question here, and that's what we relied on in our report.

His analysis of the user guides for Dominion Voting Systems and -- I don't think that -- I don't think that he was wrong in his analysis. I think we aired his statements, and we stand by them to this day.

Q. Okay. By the way, this piece that got -- made

it into the reporting, it was shown, it looked to me, like maybe a second as you were talking about Mr. Krebs.

You never actually reported on Dominion's position during the portion of this report where you were showing Exhibit 61 to your audience, did you?

MR. RHODES: Objection. Misstatement -- misstates the facts.

A. Mr. Cain, I think I showed this screen several times, at least twice, I believe, in my special.

Q. (By Mr. Cain) Okay. Let me -- let me look at the one. If we have time, I'll see if I can find one of them.

The one I was thinking about, Ms. Rion, was the one towards the end, where you showed a quick piece of Mr. Krebs. I think it's around the 26-minute mark.

This is the part you're talking about the other employee at Dominion; right?

A. Correct. Penelope Chester Star. She had -- she was vice president at TENIA (phonetic). the organization affiliated with --

(The video segment was played.)

Q. (By Mr. Cain) So is that one of the examples of when you put up the Dominion FAQ page?

A. It is.

Q. Let me ask you this: There was a statement that

Mr. Oltmann made a little earlier in this when we were playing his interview. And I'll just finish with this statement. I want to hear your response to what he had to say at about 23:30.

(The video segment was played.)

Q. (By Mr. Cain) Actually, time out on that.

You never got any actual documentation -- I know you requested it, but you never got any documentation of his status as a shareholder of the company; right?

A. Correct. That statement was based off of summarizing what Mr. Oltmann had told me in our interview.

Q. But you did ask him for it; right?

A. I did. But I had no reason not to believe that statement when he did not produce those documents.

We were -- at this point, I had interviewed -- I think I have interviewed him for about 20 minutes, I think. And we talked about various topics. But I had asked that, I think, in retrospect via email.

Q. Okay. My question was you just never got -- you actually never got written confirmation of that?

A. No. No written confirmation. Just relying on Mr. Oltmann's account of that. And, you know, we had no reason not to believe him at this point.

(The video segment was played.)

Q. (By Mr. Cain) So you would agree with me there,

what you put Mr. Oltmann's -- well, let me -- let me back up.

You had ability to edit what was going to be in the interview or in the final broadcast or not; right?

A. Yes.

Q. And you, in that process, decided to leave in the statement that Mr. Oltmann just made that Eric Coomer was responsible for putting his finger on the scale; correct?

MR. RHODES: Misstates the recording.

Q. (By Mr. Cain) You can answer it.

A. Mr. Cain, I believe he's -- that was stated by Mr. Oltmann in context of the Antifa call that he was participating in.

I believe, in the interview, he says that the participants of these Antifa calls were usually people who just, kind of, talked and maybe did not -- did not really have the power to act.

And in this case, considering Dr. Coomer's role at Dominion Voting Systems and his education and his title, he was capable -- more capable than the other, I guess, Antifa members on the call.

So I think that's what he meant by that.

Q. Let me -- let me back it up and make sure that I didn't mishear it. Then we can conclude.

(The video segment was played.)

Q. (By Mr. Cain) And you stand by your -- your last statement after hearing that again?

A. Yes. He just said he's just not -- he's not just a member of Antifa; he had the ability beyond just being a -- you know, throwing bottles of urine at Secret Service in front of the White House.

MR. CAIN: Okay.

Well, ma'am, I appreciate your time here today. And I'm probably at my three-hour mark, so I'll -- I'll conclude. Thank you.

THE WITNESS: Thank you, sir.

MR. RHODES: Charlie, you want to take the share screen down, please?

MR. CAIN: Are you going to do the same thing on this one?

MR. RHODES: Yes.

MR. CAIN: Let me make a record. Also, understand we've got another deposition.

So before Mr. Rhodes starts, I understand, based on the discussion -- or the questions with Mr. Herring that Mr. Rhodes believes he can ask questions of his client and somehow present that to the Court.

I'm certainly not afraid of any question,s but I think it runs afoul of the Court's order, and I think it

runs afoul of my obligation present to prima facie evidence of my claims.

And it also suggests that additional testimony would be submitted by the defendants to try to contradict those claims, and I don't believe that's in accordance with how the Court should weigh the evidence.

And I understand you disagree with that, Mr. Rhodes. So go ahead and make your record, and, hopefully, it won't be too long.

MR. RHODES: Thank you.

MR. ZAKHEM: Excuse me. This is John Zakhem. I am counsel for the Trump Campaign.

I understand that, per the scheduled notice, my client's 30(b)(6) deposition to begin in under 15 minutes. We have -- I have availability only until about 5:15 p.m., Mountain Time, accounting for a couple of breaks on the three-hour limitation, at which time I will not be able to continue with any deposition.

So I just want to make the parties aware of that and let everybody know I'm getting off, and so is my client, no later than 5:15 this afternoon.

I'm happy to make accommodations for additional time according to the availability of the respective parties and counsel. And if it may be more appropriate to continue Ms. Rion's deposition to a later time to

accommodate the questions from her counsel, that may be more efficient in order -- because I don't intend on asking any questions of my client in its deposition.

But I wanted, Charlie, you to be aware of what's going on here, because I'm on a very, very tight schedule.

MR. CAIN: Thanks, John. I don't think you should have to worry about it, because I don't think we need to spend time asking questions.

I would make the request, Mr. Rhodes, that we conclude this deposition so that we can get to the Trump Campaign and get it finished, given the limitations, and then just talk about, maybe, resolving this at a different date. But I think we need to move on.

MR. RHODES: I disagree. If you -- if you want to reschedule the Trump deposition --

MR. CAIN: Absolutely not.

MR. RHODES: -- I have no objection to that.

MR. CAIN: No. You can't -- you know, your codefendant is asking and saying that they have a limitation. And we really need move on to that deposition.

I think it's unfair to put us in a position of limiting a noticed deposition with this type of questioning.

MR. RHODES: I did not notice either deposition;

you did, Mr. Cain. And you have co-counsel, who, by the way, when he finishes a deposition in this case, says, "Pass the witness." And then cross-examination is done, and then he does redirect examination, Mr. Cain.

CROSS-EXAMINATION

BY MR. RHODES:

Q. So Mr. Rion -- Ms. Rion -- excuse me -- let's start with where we ended.

I'm showing -- going to share my screen.

MR. CAIN: Can I interject real quick?

John, can I -- can I talk with you offline while he goes through this? I'll get your cell phone.

MR. ZAKHEM: Yeah. Let me just -- let me just give it to you on the record. Are we on the record?

MR. CAIN: We still are.

THE REPORTER: Yep.

MR. ZAKHEM: Can we go off the record briefly?

I'll give you my cell phone. I don't want that on the record. And just call me. I'll bounce off of the call, or off the depo.

THE VIDEOGRAPHER: Going off the record. The time is --

MS. DOMINGUEZ: I can put you both in a breakout room if you'd like.

MR. CAIN: Just give us the number. We'll do it

that way. Let's go off the record.

THE VIDEOGRAPHER: Going off the record. The time is 3:49.

(Discussion off the record.)

THE VIDEOGRAPHER: We are back on the record. The time is 3:49.

Q. (By Mr. Rhodes) Ms. Rion, do you see Exhibit 61?

A. Yes.

Q. You were just asked about this, and you were asked about -- Mr. Cain asked you about two organizations. He said The Department of Homeland Security and the Cybersecurity Infrastructure Security Agency.

But you see, in fact, there's an apostrophe S after "Homeland Security"; correct?

A. Correct.

Q. And so your statement was that CISA, and Mr. Krebs in particular, had walked back this statement to some extent in a later tweet. Is that -- was that -- did I understand you correct?

A. Correct. I believe -- I believe it was a November 18 tweet. I'm -- I'm sorry. I don't recall it verbatim.

Q. I'm going to show you what I am marking as Exhibit OAN O.

(OAN Exhibit O was introduced.)
Q. (By Mr. Rhodes) Is Exhibit O the tweet that you were referring to from Mr. Krebs?
A. Yes, sir.
Q. Quote, "I have never claimed that there wasn't fraud in the election, because that's not CISA's job. It's a law enforcement matter"; correct?
A. Correct.
Q. Now, going back to Exhibit 61, there is a statement by Dominion that "Dominion is a nonpartisan U.S. company." Do you see that?
A. Yes.
Q. Well, if you scroll all the way down, you'll see this page says its copyright 2020 by Dominion Voting Systems Corp. Do you see that?
A. Yes.
Q. And you told us you thought that Dominion Voting Systems was a Canadian corporation, and you said you thought you'd looked at the certificate of incorporation or something; correct?
A. Yes.
Q. I'm going to show you what I am marking -- here we go -- what I'm marking as Exhibit P.
(OAN Exhibit P was introduced.)
Q. (By Mr. Rhodes) Can you see Exhibit P?

A. Yes.
Q. I see it lists Dominion Voting Systems Corporation. That's -- that's the name that we just looked at on the statement; right?
A. Yes.
Q. It says the jurisdiction is Ontario. And you understand Ontario to be a province in Canada, don't you?
A. I do.
Q. Are you aware of any jurisdiction in the United States called Ontario?
A. No, sir.
Q. And the corporation type is an Ontario business corporation, and that it's active; correct?
A. Correct. And there is an address, I believe, right below that: Toronto, Ontario, Canada, Suite 200.
Q. Why would Dominion Voting Systems Corporation issue a statement that they're a U.S. corporation when it's plain they're a Canadian corporation? Do you know?
MR. CAIN: Objection. Leading. Objection. Form.
A. I -- I don't know. I assume that they -- it's better for their -- their fact sheet for them to be able to say that they're a U.S. company.
MR. ARRINGTON: This is Barry Arrington. I see that it's five minutes until the next deposition is

scheduled. I, obviously, can't be at two place at one time.
Has there been a resolution? Are we just going to finish this one and start the Trump Campaign one? Or, Charlie, can you fill me in on that?
MR. CAIN: We're going to finish this one and then start five minutes after this one finishes, assuming we can get all that coordinated with the court reporter.
And then John and I have a separate agreement, but we can talk about that later.
MR. ARRINGTON: Okay. Thank you.
Q. (By Mr. Rhodes) You were also shown Exhibit 56, the DEF CON report. Do you recall that?
A. Yes.
Q. And this is something you looked at in connection with "Dominion-izing the Vote"; is that correct?
A. The DEF CON 27 report, I believe.
Q. I'm showing that to you now.
A. That's the one.
Q. Okay. You were asked about Matt Blaze. You said you did not know Professor Blaze; correct?
A. Correct.
Q. But then Mr. Cain showed you another document, which we'll look at, in which Professor Blaze said that

he's not aware of any hacking that occurred in the 2020 election; correct?
A. Correct.
Q. You see there's -- there's other academics here -- Mary Hanley from the University of Chicago, Rachel Wehr from Georgetown, Kendall Spencer from Georgetown, Christopher Ferris from Georgetown. Do you see these people?
A. Yes.
Q. I'm going to show you Exhibit 58, which Mr. Cain showed you. And fortunately for us, these people put their name in alphabetical order.
So the first one I mentioned is Mary Hanley. Let's see. That would be -- L, M -- that would be somewhere between 22 and 23. Do you see Mary Hanely from the University of Chicago on here?
A. I do not.
Q. Then there's Rachel Wehr, W-e-h-r. That'd be between 55 and 56. Do you see her on here?
A. No.
Q. Then I see Kendall Spencer -- S-p. Oh, Specter. We're close. Spencer, I guess, would be 46 and 47. Do you see him on here?
A. No.
Q. Christopher Ferris, F-e. That'd be between 18

and 19. Do you see him on her -- him on here?
A. No, sir, do not.
Q. So these experts haven't said anything about them believing that there's nothing happening to the 2020 election, have they?
MR. CAIN: Objection. Goes to the weight of which -- you cannot create a fact issue on that topic. Irrelevant, as is all of this.
Q. (By Mr. Rhodes) Go ahead, Ms. Rion.
Those individuals haven't said that there was no hacking of the 2020 election, have they?
A. It appears not. And they have not endorsed this letter. It seems they haven't.
MR. CAIN: Objection. Responsiveness.
Q. (By Mr. Rhodes) Okay. Let's go back to Exhibit 56, the DEF CON report.
Now, I did Mr. Watkins tell you about this document?
A. No. I found this document on my own. I -- I don't remember how I -- (audio interference) -- not this particular report, but I know DEF CON was referenced in the HBO series -- film Kill Chain. But I found DEF CON 27, this particular report, on my own.
Q. And I'm directing your attention to the Bates Number 1632, page six. When it just gives an

executive summary and says, "Every piece of equipment at the Village is currently certified for use in at least one U.S. jurisdiction"; correct?
A. Correct.
Q. "And once again, Voting Village participants were able to find new ways or previously published methods of compromising every one of the devices in the room in ways that could alter stored vote tallies, change ballots displayed to voters, or alter the internal software that controls the machines.
"In many cases, the DEF CON participants tested equipment they had no prior knowledge of or experience with and worked with any tools they could find in a challenging setting with far fewer resources and far less time than a professional lab or even the most casual attacker would typically have"; correct?
A. Correct.
MR. CAIN: Let me interject.
It's 2:01. It's a minute past the notice time for the Trump Campaign deposition. Plaintiff reserves its right to seek expenses, costs, and attorneys' fees associated with this delay.
Q. (By Mr. Rhodes) I want to now turn to page 123, Bates Number 1638. This is a listing of the items that were tested, and among them is the Dominion ImageCast

Precinct; correct?
A. Correct.
Q. And the results of that testing start on page 20; correct?
A. Yes.
Q. And it states that "The Dominion ImageCast Precinct is an integrated hybrid voting system. Participants were able to access USB, RG45, and CF," -- compact flash -- "slots on this machine without using destructive force"; correct?
A. Yes.
Q. "The system also runs Busybox Linux 1.7.4, which has twenty currently known medium to high level vulnerabilities, including the ability to allow remote attackers to gain access"; correct?
A. Yes.
Q. The next page, page 21, Bates Number 1647: "As a group, they were able to boot an operating system of their choice and play video games on the voting machine, including a popular game called 'Pong'"; correct?
A. Correct.
Q. You were aware of that while you were preparing "Dominion-izing the Vote"?
A. Yes, I was.
Q. You were aware of that fact when you interviewed

Ron Watkins and he explained the vulnerabilities to you?
A. Yes, I was.
Q. Now, you also said that Mr. Watkins provided you almost a thousand pieces of -- a thousand pages of documents; correct?
A. Yes. About -- about a thousand.
Q. Including the user manuals for Dominion; correct?
A. Correct. I believe there were two. One was a -- I forget what was second one was, but they were, at the end of the day, user manuals for Dominion Voting Systems.
Q. I'm going to mark as the next exhibit --
(OAN Exhibit Q was introduced.)
Q. (By Mr. Rhodes) I've marked as Exhibit Q the Dominion Democracy Suite ImageCast Central User Guide. You see that?
A. I see it.
Q. Mr. Watkins provided this to you?
A. Yes, he did. It was a link that was -- I think it was publically available.
Q. All right. It want to direct your attention to page 16, at the bottom, OAN 782, and the chapter three.
There's the Administrator mode, and then there's "Supervisor mode is a high-level mode reserved for

technicians authorized by Dominion Voting."
Do you see that?
A. Yes, I do.
Q. And when you were discussing with Mr. Watkins the user manuals, did you have a copy in front of you?
A. I did.
Q. And you were following along with him as he was explaining things?
A. Yes, I was.
Q. And going to page 19 of the manual, Bates Number 7825. For the Supervisor mode, turning to the next page, 20, 786: "The ImageCast Central's advanced settings allow for adjustment of the scanning properties with the application in Supervisor mode."
Do you see that?
A. I do.
Q. And among those settings I highlighted here is the gamma setting.
A. Right.
Q. Is that consistent with what Mr. Watkins told you?
A. It is very consistent with what he told us.
Q. And on the next page, page 21 of the report, Bates Number 787, again, a reference to the brightness, contrast, and gamma levels; correct?

A. Correct.
Q. Mr. Cain asked you, Well, who can adjust those settings? And the answer is, Only somebody that Dominion has given permission to; correct?
A. Correct.
Q. And that would include Dr. Coomer?
A. Yes.
Q. Mr. Watkins also gave you a second manual, you said; correct?
A. Yes.
Q. I'm showing you Exhibit R.
(OAN Exhibit R was introduced.)
Q. (By Mr. Rhodes) Is this the second manual that Mr. Watkins provided you, the Democracy Suite EMS Election Event Designer User Guide?
A. That was the one.
Q. And I'm showing you page 262 of the manual, Bates labeled OAN 1096, with the section titled A.11, "Changing Scanning Configuration." Do you see that?
A. Yes, I do.
Q. And then the next page, 263, OAN 1097:
"NOTE: The scanning parameters should only be changed by an advisory of the Dominion Voting Systems engineering group."
So again, in response to Mr. Cain's question,

the individuals who were able to change the scanner settings, pursuant to Mr. Watkins' theory, are only individuals at Dominion Voting Systems?
A. That's correct.
MR. CAIN: Form. Leading.
A. This is what Mr. Watkins shared with us in our interview. So we're following along in this manual, and that's -- that was reasonable to us.
Q. (By Mr. Rhodes) Was there anything Mr. Watkins told you during the interview which you -- you found contradicted in any of the nearly thousand pages he gave you?
A. Not -- not that I'm aware of.
We conducted a fairly lengthy interview with him, and we followed along with -- along with every statement he made in that interview.
(OAN Exhibit S was introduced.)
Q. (By Mr. Rhodes) I'm going to show you what I've marked as Exhibit S. This is one of the three Texas secretary of state reports that Mr. Watkins provided you; correct?
A. Correct.
Q. And you'll see on the third page, Bates Number 1162, one of the objections of the Texas secretary of state is that some of the hardware in the Democracy 5.5

system can be connected to the internet; correct?
A. Yes. That was a very central concern with these machines.
Q. And on the next page, page 4, Bates Number 1163, their discussion of "The adjudication portion of the tabulation process in which the election management software was problematic and showed that the handwritten write-ins subject to adjudication were not easily picked up by the ballot scanner.
"This poor resolution on the scanner also failed to pick up some of the printed wording on the ballots.
"In a follow-up, the vendor stated that only black Sharpie markers should be used for marking the ballots. However, when black Sharpie was used during testing, it did, on a few occasions, bleed through to the back side of the two-sided ballot in such a way that it would confuse the ballot scanner or kick the ballot out"; correct?
A. Correct.
Q. This was while you were preparing "Dominion-izing the Vote"?
A. Yes.
Q. So I want to go back to Exhibit 61 that Mr. Cain marked -- the statement from Dominion Voting Systems corporation that there are no issues with the use of

Sharpie pens.
Do you know why Dominion would say that when they have in writing from the Texas secretary of state that is there an issue with the use of Sharpie pens?
MR. CAIN: Objection. Leading. Objection. Form.
A. It was one of the aspects that we looked at, and -- and it caused -- causes one to question every other fact-checking element that Dominion Voting Systems was putting out.
So I don't know why they would have issued that statement, given the problems that were existing in, at least, Texas.
Q. (By Mr. Rhodes) And -- and by the way, you said that by the time of your tweet on November 17th, Eric Coomer and his "Don't worry. I made F-ing sure of it," were trending on Twitter; correct?
A. For several days, it was trending on Twitter, I think right after Michelle Malkin's interview.
Q. Is there anything in Dominion's statement coming to the defense of Mr. Coomer?
A. No. That was -- there does not seem to be any mention of Eric Coomer in this statement, which was very odd to us considering Eric Coomer was, arguably, one of the number-one controversies involving Dominion systems at

the time they issued this statement.
So we've -- that was -- that was very odd to us. It -- it seemed to indicate that Dominion was -- knew of -- I mean, they -- they clearly didn't address Dr. Coomer.
So I don't -- it was -- it was very unusual, considering the profile that Eric Coomer was building in the public sphere.
MR. CAIN: Objection. Responsiveness, and to the entire line of questioning, and to the campaign witness now sitting for 15 minutes.
(OAN Exhibit T was introduced.)
Q. (By Mr. Rhodes) I'll show you what I've marked as Exhibit T. This is the second of the Texas secretary of state reports that Mr. Watkins provided you; correct?
A. Correct.
Q. And on the second unnumbered page, Bates Number 1166, under Findings: "Examiner reports raise concerns about whether the Democracy Suite 5.5 is suitable for its intended purpose, operates efficiently and accurately."
You knew that when you were preparing "Dominion-izing the Vote"; correct?
A. Yes.
Q. You knew that when you were assessing the

credibility of Ron Watkins; correct?
A. Correct.
Q. And is there anything about these statements from the Texas secretary of state that would cause you to think that Mr. Watkins didn't know what he was talking about?
A. The statement -- the report seems to confirm what Mr. Watkins relayed to us, and that's -- that was part of our assessment.
(OAN Exhibit U was introduced.)
Q. (By Mr. Rhodes) I'll show you what I've marked as Exhibit U. Do you see that?
A. I do.
Q. On the first page: "A distinguishing feature is the extensive use of commercial off-the-shelf components, or COTS components, to use the industry parlance. COTS components are standard hardware or software products, as opposed to custom-made components.
"For example, the D Suite voting terminals are commercially available Android tablets that include the stand and the smartcard reading used for voter authentication.
"Similarly, the PCs, networking gear, hard drives, printers, and some scanners are COTS components"; correct?

A. Correct. Like Windows Operating System 10, I believe. This was --
Q. And is that consistent, again, with what Mr. Watkins told you?
A. It matches up exactly.
Q. Turning to page three of the third Texas secretary of state report, Bates Number 1170, Problems Identified: "Adjudication results can be lost. In the January exam, during adjudication of the ballots in the test election, one of the Dominion representatives made a series of mistakes that caused the entire batch of adjudication results to be lost."
Again, is that consistent with what Mr. Watkins told you?
A. Yes.
MR. CAIN: Objection. Form. Objection. Leading.
(Audio interference) challenging the Texas vote? I missed that part of the case.
MR. RHODES: You didn't -- you didn't miss that part of the case, Mr. Cain. You choose to ignore that part of the case.
Q. (By Mr. Rhodes) Next, look at page 4, OAN 1171, Test Voting: "During our voting test, we discovered that some party names and proposition texts were not displayed,

and one scanner was not accepting some ballots. These all turned out to errors Dominion made in setting up the standard test election used by the secretary of state.

"In the case of the scanner, it had actually been configured not to accept machine-marked ballots."

And scanner configurations, we know, are left to Dominion; correct?

A. Correct.

Q. We saw that in the Dominion manual.

A. Yes.

Q. Is this -- is this fact here about the Dominion software failing the test voting in Texas something that, in your mind, added to your belief in the credibility of Mr. Watkins?

A. Absolutely. It was -- this was particularly relevant to us.

Q. Page 5, Bates Number OAN 1172:

"USB Port Vulnerability. The ICX ballot-marking device has an indicator light on top to show poll workers when the station is in use. That light is connected by a USB port.

"When Brian Mechler's phone was attached to the USB port, the ICX scanned the files on his phone and did not complain; although Dominion later showed the event was logged.

"When a USB drive with files was inserted, the ICX sometimes complained and sometimes did not, apparently according to the contact of the USB drive and whether it was present when the ICX was first powered up or inserted later."

Again, was this an issue that Mr. Watkins explained to you was a vulnerability, was the accessibility of ports on the Dominion system?

A. It was.

And furthermore, that was confirmed in the DEF CON 27 report, where hackers were able to access these USB drives without having to tamper or struggle with the machine. It was fairly accessible. So all of this corroborated Mr. Watkins' statement.

(OAN Exhibit V was introduced.)

Q. (By Mr. Rhodes) I'm going to show you what I marked as Exhibit V, as in Victor, and ask you if this is a report from the Pennsylvania secretary of state which Mr. Watkins provided you and which you reviewed while preparing "Dominion-izing the Vote."

A. This is the document.

Q. And you mentioned earlier, I believe, something about part of the problem with this CO -- commercial off-the-shelf, you said, included -- I think you mentioned Windows 10; is that right?

A. Yes. A particularly vulnerable system, I understand, from those who hack for a living. They say that Windows 10 is one of the easier systems to hack into.

Q. And I'm showing you Bates Number OAN 1229. And for the Dominion Voting Systems software, you see it's a running off Windows 10 as a commercially off-the-shelf software; correct?

A. Correct.

Q. And then there's all kinds of other unmodified commercially off-the-shelf products. On the next page, 1230, virtually the whole page are unmodified commercially off-the-shelf products.

Oh. And I see there's a -- there's a reference to the aerial fonts.

A. Yes.

Q. Did that strike any bells with you?

A. Of course. That was actually one of the pieces of -- or one of the concerning elements for Mr. Watkins, was the fact that, in aerial, you have the capital letter I and the letter -- the lowercase letter L look exactly the same. So you could potentially write "Repubican" versus "Republican".

The reason that is relevant is that you could, potentially, have marked President Donald J. Trump as "Repubican," and then the rest of the Republican

candidates as "Republican," using the correct L.

And that would have allowed for those Republican candidates to have registered -- their votes to have been registered, but Donald Trump's votes to have been, potentially, tossed aside, which would explain, as Mr. Watkins laid out for us, why, in some precincts, Donald Trump did not perform as well as the down-ballot ticking for the rest of the Republicans on the ballot.

Q. So -- so Mr. Watkins' story was corroborated down to the font?

A. Down to the font.

Q. The next page, OAN 1231, I see we have commercial off-the-shelf. We have Dell, Dell, Dell, Dell, Dell, Dell, Canon, Canon --

A. Right.

Q. -- Dell, Dell, Dell, HP, HP, Dell, Dell, Dell, Dell, Dell, Dell; right?

A. Right.

Q. All things that Mr. Watkins told you was concerning to him?

A. Correct.

Q. And the same thing on page 1232; correct?

A. Correct.

Q. Mr. Watkins also provided you with the. Calhoun County, Michigan, ICC User Manual; correct?

A. Yes, he did.
Q. I've marked that as Exhibit W.
(OAN Exhibit W was introduced.)
Q. (By Mr. Rhodes) All right. Can you see Exhibit W?
A. Yes, I can.
Q. And turning to the second page, there's instructions to open the file explorer, select "This PC." This looks remarkably similar to the Windows folder system; correct?
A. It does, yes. And, plus, there's the One Drive, which also indicates it's a Microsoft system.
Q. Okay. Yeah. Oh. Okay.
Again, is this something that Mr. Watkins told you, is that this system simply runs on a Windows file system?
A. Yes. This was consistent with what he told us and raised a red flag for him.
Q. Because anyone can just go in and move folders around?
A. Correct. It's a matter of copy, pasting, or clicking and dragging a folder from one spot to the next.
Q. And then, also, you mentioned the reference to One Drive. What is One Drive?
A. One Drive is a cloud, I guess, storage system

from Microsoft.
Q. So these systems are actually, in purpose, set out -- designed to connect to the cloud?
A. Yes. You can't use One Drive without connecting to the internet.
Q. So when Dominion says, Oh, they don't connect to the internet, that -- that's not consistent with the documents Mr. Watkins provided you, is it?
A. No, sir. That's right. Not consistent.
Q. You were asked whether or not you were -- whether you asked Mr. Oltmann for a copy of his notes. Do you recall that?
A. Yes.
Q. Have you seen his notes?
A. Not before putting out this report.
Q. Have you since seen them?
A. I have.
Q. I'm going to show you what's previously been marked as Plaintiff's Exhibit 29.
And in particular, I'm directing your attention to the second page, where it says, quote, "Trump not going to win. I made F-ing [sic] sure of that," closed quote.
If you had seen these notes prior to broadcasting "Dominion-izing the Vote", would they have change were changed your report in any way or --

A. No, they would not have.
Q. Are these notes consistent with what Mr. Oltmann told you?
A. Yes.
MR. CAIN: Form. Leading.
Q. (By Mr. Rhodes) You told Mr. Cain, I believe, when he showed you -- well, here. We'll do it. We'll pull up Exhibit 60.
I'm showing you Exhibit 60, which Mr. Cain marked. This is Mr. Watkins' tweet on, it says, November 3rd: "Ms. Chanel Rion just reached out to me, and I'll be talking with her about Dominion tomorrow"; correct?
A. Correct.
Q. Well, I think you previously testified that you were not aware of Mr. Oltmann or Mr. Coomer until on or after the Michelle Malkin interview on November 13.
A. That's correct.
Q. So, I mean, did Mr. Oltmann send you to Mr. Watkins?
A. No. I found Mr. Watkins before even -- I even knew about Eric Coomer or even heard of Michelle Malkin's interview.
Q. So you independently found Mr. Watkins and independently determined his credibility. You did not

rely on anything Mr. Oltmann told you?
A. Absolutely.
Q. You were asked about did you have contact with the Trump Campaign, Rudy Giuliani, or Sidney Powell. And you said, Yes, in connection with setting up interviews; is that correct?
A. That's correct.
Q. I just want to clarify: Other than setting up -- attempting -- attempting to set up or actually setting up interviews in connection with "Dominion-izing the Vote", did you have any other -- any other contact with anybody from the Trump campaign, Rudy Giuliani, or Sidney Powell?
A. I'm going to step outside for a quick second, but I'm going to answer your question. Sorry.
So to answer your question, no. I -- I recall setting up interviews. And oftentimes, over the course of being a -- working as a journalist, I will often send information to my interviewees either to confirm a fact or to get their statement on it.
So that's the extent of other correspondences you may have -- you may see from me to the Trump Campaign.
Q. Did -- did -- did anyone from the Trump Campaign or Rudy Giuliani or Sidney Powell review "Dominion-izing the Vote" before it aired?

A. No.
Q. Did you share any portions of the script with them?
A. No.
Q. Did they have any input into what went into it, other than Mr. Giuliani appearing for a -- an interview?
A. No.
Q. You were asked whether or not Mr. Oltmann was a conservative activist, and you said "Yes."
A. Yes.
Q. And then you were asked, Did that make a difference to you? And you said, "Yes." What did you mean by "Yes"?
A. I meant that, in confirming that Mr. Oltmann was actually working to identify Antifa radical leftist elements in his community and was an activist, in that he was exposing journalists who had Antifa affiliations, this made sense that he was conservative activist, and that confirmed his bona fides, if you will, as an Antifa exposer.
Q. Okay. You're not suggesting that merely because he's conservative, he's credible?
A. Oh, no, no. That his conservatism confirmed that he was, in fact, investigating or at least looking into Antifa and trying to expose them -- a leftist

organization or group.
Q. And you also mentioned in your examination by Mr. Cain that you were familiar with conference calls or Zoom calls by other leftist organizations; correct?
A. Correct. I believe -- I believe I -- I was doing a story on the Sunrise Movement, for example. This was a group of federal employees who were convening a conference call.
And in these conference calls, they were figuring out ways they could act out their rage and create -- sow disorder and chaos in Washington, D.C. and elsewhere.
Q. I'm going to show you what I've marked as Exhibit X. And tell us what this is, please.
(OAN Exhibit X was introduced.)
Q. (By Mr. Rhodes) Let's hope you can see this, because optimizing screen sharing does not come through.
(The video segment was played.)
Q. (By Mr. Rhodes) Could you hear that?
A. Yes.
Q. And what is that report?
A. That report was on leftist group that was colluding on phone calls, conference calls. And they were discussing ways to sow chaos and discord in Washington, D.C. They were anti-Trump,

Antifa-sympathizing anarchists.
Q. And that was prior to the election. I believe that was on November 2nd; correct?
A. Yes. I believe that was one day before the election.
Q. So when you heard that Mr. Oltmann said that he'd infiltrated an Antifa call, was that -- did you find that credible based upon your personal experience?
A. Yes. That was -- it did not seem unreasonable that Antifa as a group was coming together and making plans as a group.
Q. You also told Mr. Cain, I believe -- you couldn't quite remember the name of it, but you had reviewed an article -- I'm showing you Exhibit A -- in Colorado Politics.
A. That's right.
Q. And this is, again, Mr. Oltmann stating that his intent was to identify Antifa reporters long before any information came out about Eric Coomer; correct?
A. Correct.
Q. You also said that you had looked into his business -- by "his," I mean Mr. Oltmann's, business, the PIN Business Network.
Let me show you what I've marked as Exhibit Y.
(OAN Exhibit Y was introduced.)

MR. CAIN: And I'm going to renew my objection that if you want to question her some more, we do it at a later day. The Trump Campaign witness has now been sitting for 42 minutes after we noticed his deposition.
So I would ask, Bernie, that you put a bookmark in this, and we can deal with it later.
MR. RHODES: I'm almost done, if the network will cooperate.
Q. (By Mr. Rhodes) Let's try this. I'm going to show you my copy of what I'll represent to you is marked as Exhibit Y. Do you see this?
A. Yes.
Q. From the P-I-N, PINbusinessnetwork.com, "Who Are We?" And that's Mr. Oltmann as the president; correct?
A. Correct.
Q. And it goes on to show -- I don't know -- more than 50 people?
A. Yes.
Q. Was that significant to you?
A. It was. It showed that Mr. Oltmann had -- had a business, a legitimate business, that he was not likely to throw away by stepping out and providing some kind of story that he didn't feel comfortable sharing. It was significant that he had a fairly established presence in his community.

Q. And I'll show you Exhibit Z. Hopefully this one works better.
(OAN Exhibit Z was introduced.)
Q. (By Mr. Rhodes) What is Exhibit Z, Ms. Rion?
A. This is the press release showing Oltmann was nominated, I guess, entrepreneur of the year. This corroborated what had he told us. And this is actually a press release I looked at.
Q. This is all research you did to assess Mr. Oltmann's credibility?
A. Correct.
Q. So in addition to all the other information you told us about Mr. Coomer and where you believe it was Mr. Coomer who's "Eric from Dominion," you also came to believe that Mr. Oltmann was credible?
A. Yes; that what he told us about his own background was credible, and that his motives for sitting in on this call were also -- they seemed to match up. They were reasonable.
Q. You said that as part of your investigation into Dr. Coomer, you reviewed the fact that he had six patents and another six patent applications; correct?
A. Correct.
Q. I'm showing you Exhibit AA.
(OAN Exhibit AA was introduced.)

Q. (By Mr. Rhodes) Is this a listing that you collected while preparing "Dominion-izing the Vote" of Dr. Coomer's patents and patent applications?
A. Yes. The page that you're showing me is one of them.
Q. Is one of them, yes.
So the first one, the patent is titled "Ballot Adjudication and Voting System Utilizing Ballot Images"; correct?
A. That's right.
Q. And it shows the assignee is a Dominion Voting, and one of the vendors is Eric Coomer?
A. Dominion Voting Incorporated.
Q. Okay. And then we keep going. Ballot adjudication. Ballot adjudication.
"Ballot level security features for optical scan voting machine capable of ballot image processing, secure ballot printing, and ballot layout authentication and verification."
A. Yes.
Q. "Systems for configuring voting machines, docking devices for voting machines, warehouse support, and asset traffic of voting machines."
A. Yes.
Q. If a group of hackers could play Pong on a

Dominion voting machine over a weekend, what did you believe that someone who had this knowledge of the Dominion Voting Systems could do?
A. That he could -- someone with that kind of background could access machines on a systemwide basis and, certainly, adjust the gamma settings, adjust the image settings, whatever it was that would set ballots aside for adjudication.
That was something that was feasible considering Dr. Coomer's background and invention of that actual technology.
Q. You also told us that prior to your work in preparing "Dominion-izing the Vote," you had seen Kill Chain; correct?
A. Correct.
Q. The HBO documentary Kill Chain.
I want to play just a very short piece of that, which I've marked as Exhibit AB.
(OAN Exhibit AB was introduced.)
Q. (By Mr. Rhodes) It starts at the beginning with a little bit about ESS, and then it goes into Dominion.
(The video segment was played.)
Q. (By Mr. Rhodes) You had seen this documentary prior to preparing "Dominion-izing the Vote"; correct?
A. I had.

Q. And they discussed a test they did in 2014.
I want to show you last -- I'm showing you Exhibit AC.
THE REPORTER: Counsel, is it just me, or is Ms. Rion frozen for everybody else?
MR. RHODES: She's frozen for me.
MR. CAIN: Yes. Me as well.
THE REPORTER: So she may have lost her connection.
MR. RHODES: Let me see if I can call.
Sorry. You froze for a minute. We're almost done. Can we just finish this right up?
You're froze again.
MR. ARRINGTON: Bernie, this is Barry.
Allow me to suggest that if she went from an ethernet cord to wireless, that might have compromised the bandwidth.
MR. RHODES: I think that Atlas must have been -- so she went outside.
Let's go off the record a minute while I try to reach her.
THE VIDEOGRAPHER: Going off the record. The time is 4:55.
(Recess from 4:55 p.m. until 5:05 p.m.
THE VIDEOGRAPHER: We are back on the record.

The time is 5:05.

(OAN Exhibit AC was introduced.)

Q. (By Mr. Rhodes) Ms. Rion, I'm showing you what I've marked as Exhibit AC, which is the Sworn Declaration of Eric Coomer in this case. Do you see that?

A. I do.

Q. Dr. Coomer states that he was employed by Dominion Voting Systems, Inc., beginning in 2010, and as the director of product strategy and security from 2013 until May 11 -- excuse me -- May 14, 2021. Do you see that?

A. I see that.

Q. So Dr. Coomer was responsible for Dominion's security in 2014, when the machine that was the subject of Kill Chain was hacked; correct?

A. Yes.

Q. Do you know why Dr. Coomer is no longer with Dominion?

A. I don't know why.

Q. Would you like to know why?

A. I would.

MR. RHODES: I have no further questions. Thank you.

MR. CAIN: I don't need to restate my position. We need to get on to the other deposition. So we should

conclude.

THE VIDEOGRAPHER: Going off the record. The time is 5:07.

MR. ARRINGTON: This is Barry Arrington on behalf of Michelle -- I'm sorry -- Sidney Powell. We would like our normal e-transcript.

MR. RHODES: Chanel, you can go now. Thank you.

MS. RION: Thank you.

(Whereupon, the video record was concluded.)

MR. RHODES: This is Bernie Rhodes. The same as before.

THE REPORTER: Thank you.

MR. QUINN: This is Don Quinn. We'll take the same copy.

MR. ZAKHEM: This is John Zakhem. Same thing. Digital copy.

THE REPORTER: Okay. Is there anybody else who would like a transcript?

MS. HALL: Sara, I already emailed you.

THE REPORTER: Yes. I have your order. Thank you, Ms. Hall.

MS. HALL: Thank you.

THE REPORTER: Okay. Thank you very much, everybody.

* * * * * * *

WHEREUPON, the foregoing deposition was concluded at 5:08 p.m. Total time on the record was 4 hours and 22 minutes.

I, CHANEL RION, the deponent in the above deposition, do hereby acknowledge that I have read the foregoing transcript of my testimony, and state under oath that it, together with any attached Amendment to Deposition pages, constitutes my sworn testimony.

_____ I have made changes to my deposition

_____ I have NOT made any changes to my deposition

_____

CHANEL RION

Subscribed and sworn to before me this _____ day of _____, 20____.

My commission expires: _____.

_____

NOTARY PUBLIC

REPORTER'S CERTIFICATE

STATE OF COLORADO)
CITY AND COUNTY OF DENVER)

I, Sara A. Stueve, a Registered Professional Reporter and Notary Public within and for the State of Colorado, commissioned to administer oaths, do hereby certify that previous to the commencement of the examination, the witness was duly sworn by me to testify the truth in relation to matters in controversy between the said parties; that the said deposition was taken in stenotype by me at the time and place aforesaid and was thereafter reduced to typewritten form by me; and that the foregoing is a true and correct transcript of my stenotype notes thereof; that I am not an attorney nor counsel nor in any way connected with any attorney or counsel for any of the parties to said action nor otherwise interested in the outcome of this action.

My commission expires October 26, 2024.

SARA A. STUEVE
Registered Professional Reporter
Notary Public, State of Colorado

August 12, 2021

Mr. Bernard Rhodes, Esq.
bernie.rhodes@lathropgpm.com
August 12, 2021
RE: Coomer, Eric, Ph.D. v. Donald J. Trump For President, Inc.
8/9/2021, Chanel Rion (#4691776)

The above-referenced transcript is available for review.

Within the applicable timeframe, the witness should read the testimony to verify its accuracy. If there are any changes, the witness should note those with the reason, on the attached Errata Sheet.

The witness should sign the Acknowledgment of Deponent and Errata and return to the deposing attorney. Copies should be sent to all counsel, and to Veritext at errata-tx@veritext.com

Return completed errata within 30 days from receipt of testimony.

If the witness fails to do so within the time allotted, the transcript may be used as if signed.

Yours,
Veritext Legal Solutions

Coomer, Eric, Ph.D. v. Donald J. Trump For President, Inc.
Chanel Rion (#4691776)

ERRATA SHEET

PAGE_____ LINE_____ CHANGE_____
_____
REASON_____
PAGE_____ LINE_____ CHANGE_____
_____
REASON_____
PAGE_____ LINE_____ CHANGE_____
_____
REASON_____
PAGE_____ LINE_____ CHANGE_____
_____
REASON_____
PAGE_____ LINE_____ CHANGE_____
_____
REASON_____
PAGE_____ LINE_____ CHANGE_____
_____
REASON_____

_____ _____
Chanel Rion Date

Colorado Rules of Civil Procedure

Chapter 4, Disclosure and Discovery

Rule 30

(e) Review by Witness; Changes; Signing. If requested by the deponent or a party before completion of the deposition, the deponent shall be notified by the officer that the transcript or recording is available. Within 35 days of receipt of such notification the deponent shall review the transcript or recording and, if the deponent makes changes in the form or substance of the deposition, shall sign a statement reciting such changes and the deponent's reasons for making them and send such statement to the officer. The officer shall indicate in the certificate prescribed by subsection (f)(1) of this rule whether any review was requested and, if so, shall append any changes made by the deponent.

VERITEXT LEGAL SOLUTIONS
COMPANY CERTIFICATE AND DISCLOSURE STATEMENT

Veritext Legal Solutions represents that the foregoing transcript is a true, correct and complete transcript of the colloquies, questions and answers as submitted by the court reporter. Veritext Legal Solutions further represents that the attached exhibits, if any, are true, correct and complete documents as submitted by the court reporter and/or attorneys in relation to this deposition and that the documents were processed in accordance with our litigation support and production standards.

Veritext Legal Solutions is committed to maintaining the confidentiality of client and witness information, in accordance with the regulations promulgated under the Health Insurance Portability and Accountability Act (HIPAA), as amended with respect to protected health information and the Gramm-Leach-Bliley Act, as amended, with respect to Personally Identifiable Information (PII). Physical transcripts and exhibits are managed under strict facility and personnel access controls. Electronic files of documents are stored in encrypted form and are transmitted in an encrypted fashion to authenticated parties who are permitted to access the material. Our data is hosted in a Tier 4 SSAE 16 certified facility.

Veritext Legal Solutions complies with all federal and State regulations with respect to the provision of court reporting services, and maintains its neutrality and independence regardless of relationship or the financial outcome of any litigation. Veritext requires adherence to the foregoing professional and ethical standards from all of its subcontractors in their independent contractor agreements.

Inquiries about Veritext Legal Solutions' confidentiality and security policies and practices should be directed to Veritext's Client Services Associates indicated on the cover of this document or at www.veritext.com.

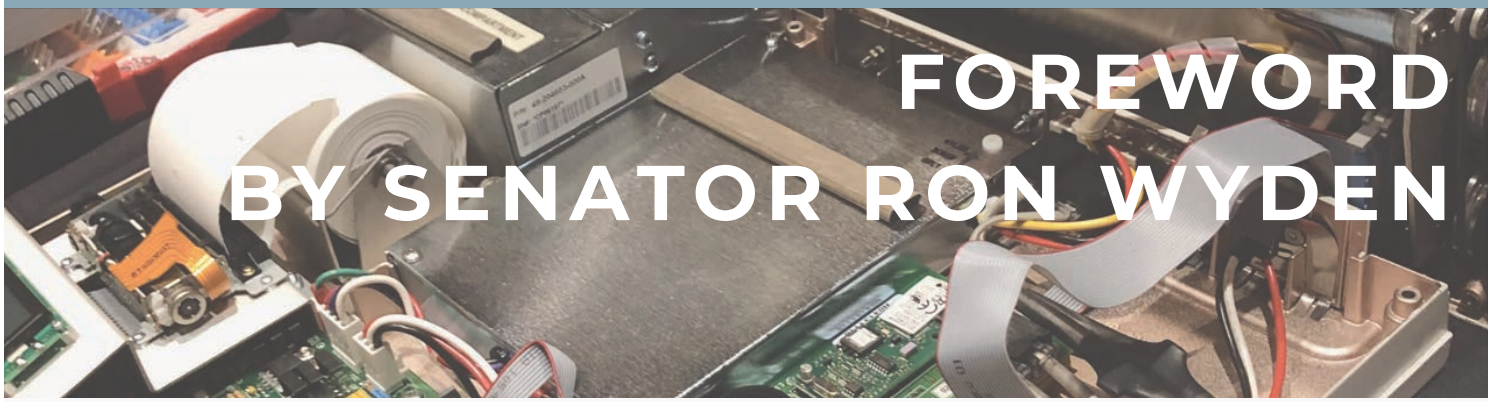
DEF CON 27 VOTING MACHINE HACKING VILLAGE

AUGUST 2019

REPORT CO-AUTHORED BY:

MATT BLAZE, GEORGETOWN UNIVERSITY
HARRI HURSTI, NORDIC INNOVATION LABS
MARGARET MACALPINE, NORDIC INNOVATION LABS
MARY HANLEY, UNIVERSITY OF CHICAGO
JEFF MOSS, DEF CON
RACHEL WEHR, GEORGETOWN UNIVERSITY
KENDALL SPENCER, GEORGETOWN UNIVERSITY
CHRISTOPHER FERRIS, GEORGETOWN UNIVERSITY

Table of Contents



FOREWORD BY SENATOR RON WYDEN

As one of the longest-tenured members of the Senate Select Committee on Intelligence, I've seen a staggering array of threats to the United States. I don't know that any threat poses more of a menace to the core of American democracy than an attack against our election system.

American democracy depends on the notion that elected representatives are chosen in elections that are free and fair, so that the government reflects the will of the people. Anything that undermines confidence in that principle strikes at the heart of our national security and identity.

And yet, nearly three years after Russia showed it was willing and able to penetrate our election systems, the hacking community at this year's Voting Village again demonstrated, our election infrastructure is still far too vulnerable to attacks.

The volunteer hackers and security researchers at the Voting Village are contributing tremendously to public understanding of how easy it is to hack our elections. Whether it is e-poll books, paperless voting machines, or ballot marking devices that print unverifiable barcode ballots, far too much of the equipment that American democracy depends is fundamentally insecure.

It doesn't have to be that way.

Congress needs to set mandatory federal security standards for our election infrastructure, from voter registration databases, to election day equipment, to election-night reporting websites. Otherwise, we're leaving state and county officials on their own against the full might of foreign government hackers. That's not a fight they should be expected to win.

In the short term, there are a handful of steps we can take to vastly improve election security. The first is reducing our dependence on insecure election equipment. Maybe, someday, there will be electronic voting machines that can stand up against dedicated hacking campaigns. That day certainly won't arrive in time for the 2020 elections, or the 2022 elections, for that matter.

As I said during my Voting Village visit last month, "We need paper ballots, guys."

Experts agree that handmarked paper ballots and post-election, risk-limiting audits provide the foundations of a secure election system. If our government takes action in the coming months,

there will still be time to dramatically improve our election security by 2020. The House has already passed a bill to ensure every voter can vote with a hand-marked paper ballot. And the Senate companion to the SAFE Act does even more to secure every aspect of our election infrastructure.

The danger is real. The solutions are well-known and overwhelmingly supported by the public. And yet the Trump Administration and Senate Majority Leader Mitch McConnell refused to take any meaningful steps to secure our elections. It's an appalling dereliction of duty that leaves American democracy at risk. These politicians need to hear the message that Americans won't accept doing nothing as the response to the serious threat of foreign interference in our elections.

The hackers at DEF CON's Voting Village did their job. Now it's time for the Senate and the president to do theirs.

INTRODUCTION

The Voting Machine Hacking Village (Voting Village) returned to DEF CON in August 2019 with a dramatic expansion in election equipment research and evaluation. DEF CON, the world's largest and best-known hacker conference, brings together a wide range of attendees including hackers; cybersecurity professionals; journalists; academics; lawyers; and local, state and federal government leaders. The Voting Village, now in its third year, saw a dramatic increase in attendance and participation, particularly from state, local, and federal government officials.

Since its launch in 2017, the Voting Village has served as an open forum to identify vulnerabilities within the U.S. election infrastructure and to consider solutions to mitigate these vulnerabilities. This year, the Voting Village demonstrated the role that hackers and other cybersecurity experts can, and should, have in the national endeavor to improve election security.

Over the course of two and a half days, hackers, technologists, academics, and other experts had full access to over 100 Voting-Village-owned voting machines to study, as well as the opportunity to attend talks and panels on topics ranging from the challenges involved in reporting on election security to the types of risk-limiting audits.

The clear conclusion of the Voting Village in 2019 is that independent security experts and hackers are stepping into the breach - providing expertise, answers, and solutions to election administrators, policymakers, and ordinary citizens where few others can.

While the discovery and replication of voting system security vulnerabilities are critical tasks for which the Voting Village plays an important role, that is not, in our view, its main contribution. Hundreds of security experts passed through the doors over the course of the weekend, many of whom had no previous experience with the particular problems and risks inherent to election technology. It is vital that we expand the pool of security experts equipped with the specialized knowledge required to evaluate, and ultimately improve, voting system security. We are especially proud of the success of the Voting Village in this essential education and outreach role.

From the outset, the mission of the Voting Village has been to highlight vulnerabilities in election equipment used in the United States and throughout the world and to serve as a resource for those whose goal is to improve the state of election security. As Voting Village organizer Harri Hursti emphasized, "As always we welcome everyone, but especially we welcome officials. We are here to help and get everyone informed - and let everyone experiment to verify the facts."

EXECUTIVE SUMMARY

1. Commercially-Available Voting System Hardware Used in the U.S. Remains Vulnerable to Attack

As in previous years, the 2019 Voting Village presented a range of currently marketed touch-screen direct recording electronic (DRE), optical scan paper voting devices, paper ballot marking devices (BMDs) and electronic poll books (e-poll books). While the Village did not attempt to (and could not) provide samples of every piece of voting equipment currently in use throughout the United States, every piece of equipment at the Village is currently certified for use in at least one U.S. jurisdiction.

And once again, Voting Village participants were able to find new ways, or replicate previously published methods, of compromising every one of the devices in the room in ways that could alter stored vote tallies, change ballots displayed to voters, or alter the internal software that controls the machines. In many cases, the DEF CON participants tested equipment they had no prior knowledge of or experience with, and worked with any tools they could find - in a challenging setting with far fewer resources (and far less time) than a professional lab (or even the most casual attacker) would typically have. In most cases, vulnerabilities could be exploited under election conditions surreptitiously by means of exposed external interfaces accessible to voters or precinct poll workers (or to any other individual with brief physical access to the machines). In particular, many vectors for so called "Advanced Persistent Threat (APT)" attacks continue to be found or replicated. This means that an attack that could compromise an entire jurisdiction could be injected in any of multiple places during the lifetime of the system.

As disturbing as this outcome is, we note that it is at this point an unsurprising result. It is well known that current voting systems, like any hardware and software running on conventional general-purpose platforms can be compromised in practice. However, it is notable - and especially disappointing - that many of the specific vulnerabilities reported over a decade earlier (in the California and Ohio studies, for example), are still present in these systems today.*

* See California Top-to-Bottom Review (2007): "Top-to-Bottom Review." California Secretary of State. Accessed September 26, 2019. https://www.sos.ca.gov/elections/ovsta/frequently-requested-information/top-bottom-review/. and
Ohio EVEREST (2007): McDaniel, Patrick, Matt Blaze, Giovanni Vigna, Joseph Lorenzo Hall, Laura Quilter, Kevin Butler, William Enck, et al. "EVEREST: Evaluation and Validation of Election- Related Equipment, Standards, and Testing." Secretary of State of Ohio, December 7, 2007. https://www.eac.gov/assets/1/28/EVEREST.pdf.

2. There is an Urgent Need for Paper Ballots and Risk-Limiting Audits

It is beyond the current and foreseeable state of the art to construct computerized (software and hardware based) voting devices that effectively resist known, practical forms of malicious tampering. However, this need not mean that elections must forever be vulnerable to compromise. Certain classes of voting equipment, including some (but not all) of the devices displayed at the Voting Village, can still be used to conduct high-integrity elections— in spite of their vulnerabilities — by conducting statistically rigorous post-election audits. Whether this is possible depends on the specific category of voting technology in use and, critically, whether a properly designed post-election audit process is routinely performed as a part of every election.

Systems that use paper ballots, such as optical scan voting devices, are physically designed to preserve a voter-marked record of each voter's intended choices (the original paper ballots themselves) which cannot be altered by even the most maliciously compromised software. These paper ballots are a prerequisite for the use of routine post-election Risk Limiting Audits (RLAs), which are a state-of-the-art, statistically rigorous technique for comparing (by human eye) a sample of ballots with how they were recorded by machine. This allows us to reliably determine the correct outcome of even an election conducted with compromised machines.

In particular, we emphasize that these audits can only be performed on paper-ballot-based systems. DRE ("touchscreen") voting devices cannot be used to conduct reliable or auditable elections in this way, because the stored vote tallies (as well as the ballot display) are under the control of precinct voting machine software that can be maliciously altered (in both theory and practice). The experience of the Voting Village strongly reinforces the widely understood risk that these machines might be compromised under election conditions in practice. The authors strongly endorse the recommendations of the National Academies 2018 consensus report, Securing the Vote,** that DRE voting machines, which do not have the capacity for independent auditing, be phased out as quickly as possible. This is an increasingly urgent matter, especially as foreign state actors (which may be highly motivated to disrupt our elections and which enjoy especially rich resources) are recognized as part of the threat to U.S. election integrity.

Unfortunately, the recommended practice of auditable paper ballots coupled with routine post-election risk limiting audits remains the exception, rather than the rule, in U.S. elections. While a growing number of states are already implementing paper ballots, legislation requiring routine risk-limiting audits has so far been advanced in only a few states.*** We strongly urge all states to adopt legislation mandating routine post-election risk-limiting audits. This is especially important because current optical scan paper ballot scanners (including those at the Voting Village) are known to be vulnerable in practice to compromise. Post-election audits are the only known way to secure elections conducted with imperfect hardware and software (as all modern computer-based hardware ultimately is).

** National Academies of Sciences, Engineering, and Medicine, Securing the Vote: Protecting American Democracy (Washington, DC: The National Academies Press, 2018). https://doi.org/10.17226/25120.
*** "Post-Election Audits." National Conference of State Legislatures, August 5, 2019. http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx.

3. New Ballot Marking Device (BMD) Products are Vulnerable

One of the most vigorously debated voting technology issues in 2019 is the appropriate role of paper ballot marking devices (BMDs) and how they relate to widely recognized requirements for software independence and compatibility with meaningful risk-limiting audits. Originally, BMDs were conceived of narrowly, specifically for use by voters with disabilities to assist them in marking optical scan paper ballots, bringing such systems into compliance with Help America Vote Act (HAVA) requirements for accessible voting. However, certain recent voting products greatly expand the use of BMD technology, integrating a BMD into the voting process for all voters, whether they require assistive technology or not.

As a relatively new technology, ballot marking devices have not been widely studied by independent researchers and have been largely absent from practical election security research studies. In the Voting Village this year, we had two ballot marking devices, representing two commercial models of this technology: a traditional ballot-marking device and a hybrid device. The findings only underscore the need for more comprehensive studies.

Participants in the Voting Village found that both BMD models were vulnerable to practical attack. In particular:

1. The hybrid machine outwardly appears to be a separate ballot-marking device and ballot optical scanner as two units physically integrated but architecturally separate. However, it was found that the ballot-marking device was connected to the ballot-scanning device over an internal network, and in fact was an active device in vote processing. This means that hacking the ballot marking device enables altering votes at the scanning stage.
2. Both devices stored information that could allow an attacker to compromise the secrecy of individual ballots.

The weaknesses in the current generation of ballot marking devices raises broad questions about their security and impact on overall election integrity if they were to be put into general use in elections. Aside from their potential to be maliciously configured to subtly mis-record voter choices, current ballot marking devices also offer potential avenues for election disruption via denial-of-service attacks. Voting Village participants observed that clearing many simple error situations (including those that could be deliberately induced by an attacker) required rebooting the device. This can easily create long lines at a polling place, since, as we also observed, it can take up to 15-20 minutes for these devices to complete a reboot cycle.

4. Infrastructure and Supply Chain Issues Continue to Pose Significant Security Risks

The Voting Village explored threats to election security from the supply chain. Participants continued to observe a wide array of hardware component parts of foreign origin, as well as other aspects of the supply chains for software and operational software maintenance. For example, participants found in one machine a hard-wired IP address pointing to an overseas address block.

The exact purpose and nature of whatever underlying feature used this address remains undetermined, but it underscores questions about foreign control over voting system supply chains, which should be understood to include not just the sourcing of physical hardware, but also of software and cloud-based and other remote services.

There are also significant practical issues of local election administration and resources. Local election offices are, overwhelmingly, under-resourced and under-funded, especially relative to the threats they face. Many county and local voting jurisdictions have no full-time IT staff, and many rely on outside contractors for election system configuration and maintenance. This reliance on outsourcing means that election officials often lack internal tools and other capabilities to effectively manage, understand and control their election infrastructure and as a consequence are without direct control over the security of their IT environment. With rapid deployment of new IT technology into the election infrastructure, election offices are especially exposed to remote attack (including by hostile state actors). Unfortunately, very few election offices have the resources to effectively counter this increasingly serious type of threat.

It is important to recognize that IT and cybersecurity are distinct disciplines with only a partial overlap in expertise. To promote discussion and collaboration between election officials and security specialists, the Voting Village conducted the first “Unhack the Ballot” initiative to create an opportunity for election officials to connect with, ask questions, and find answers from security specialists. This “off the record session” was held for the first time in a private room at the Voting Village.

EQUIPMENT AVAILABLE AT THE VOTING VILLAGE

Direct-Recording Electronic Voting Machines

A direct-recording electronic (DRE) voting machine allows voters to electronically cast their ballots by manually touching their choice of candidate on a screen, monitor, or other similar device. The DRE records and tallies the votes directly into its computer memory, without a paper ballot. Only some DRE models feature a Voter-Verified Paper Audit Trail (VVPAT).

Dominion: Premier/Diebold AccuVote TSx

The AccuVote TSx is a DRE voting machine manufactured by Premier Voting Solutions, later acquired by Dominion Voting Systems. The product line currently belongs to ES&S.

As of 2018, the AccuVote TSx was in use in 18 states.*

Dominion: AVC Edge

The AVC Edge is an electronic voting machine manufactured by Sequoia Voting Systems, later acquired by Dominion Voting Systems. It is a touch-screen machine with direct-recording electronic capabilities. It is activated by a smart card, and records votes on internal flash memory. Each unit contains a slot for a vote activation card. After the voter's ballot is cast, the smart card is deactivated to prevent multiple votes from being cast. Votes are subsequently documented. When polls close, the votes recorded in each machine are either physically or electronically transmitted to election headquarters.

As of 2018, the AVC Edge was in use in 10 states.**

ES&S: iVotronic DRE

The iVotronic DRE is an electronic voting system that allows voters to make their choices on a touch screen interface and records and tabulates votes in internal memory.

As of 2018, the iVotronic DRE was in use in 16 states.***

* "Polling Place Equipment - November 2018." The Verifier. Verified Voting. Accessed September 26, 2019. https://www.verifiedvoting.org/verifier/#year/2018/.

** According to survey of publicly available information conducted by DEF CON Voting Village.

*** "Polling Place Equipment." The Verifier. Verified Voting. Accessed September 26, 2019. https://www.verifiedvoting.org/verifier/.

Electronic Poll Books

An electronic poll book, also commonly called an e-poll book, is typically either a dedicated device with embedded software or a standard commercial laptop/tablet with a software application that allows election officials to review, maintain, and/or enter voter register information for an election, functions that had traditionally been handled using a paper-based system. These systems are limited to the check-in process and do not participate in counting the votes. The usual functions of an e-poll book include voter lookup, verification, identification, precinct assignment, ballot assignment, voter history update and other registry maintaining functions such as name change, address change and/or redirecting voters to correct voting location. In the states that allow same-day registration, e-poll books are also used to enter new voter information and interact with statewide voter registration systems.

ES&S: Diebold ExpressPoll-5000

The Diebold ExpressPoll-5000 is an e-poll book, designed for use by individual poll workers. It is used in precincts to check voters in before they are permitted to vote. The product line currently belongs to ES&S, but the ones used at DEF CON were models running Diebold/Premier-branded software, which is also still in use in several places in the U.S. Its operating system is a version of Windows CE, a system built by Microsoft for embedded applications.

ES&S: ExpressPoll Pollbook Tablet with Integrated Pollbook Stand

ExpressPoll Pollbook Tablet is an e-poll book designed for use by individual poll workers and is used in precincts to check voters in before they are permitted to vote. This product was introduced to the market in 2015 and consists of a Toshiba Encore 2 standard 10-inch tablet running Windows 8.1 operating system. It is mounted to an integrated stand which has an internal USB hub for connected peripheral devices like a printer, smart card reader, ethernet, extra battery and magnetic stripe reader.

Ballot Marking Devices

Ballot marking devices (BMDs) are machines that allow voters to make choices on a screen and then print out a paper ballot with the voter's choices, which is the ballot of record. The paper ballot is then hand counted or tabulated using an optical scanner (see description below). In general, BMDs should neither store nor tabulate votes, but only allow the voter to record votes on ballots that are then stored and tabulated elsewhere. Some BMDs produce paper print-outs of barcodes or QR codes instead of a voter-verifiable paper ballot, which has become a source of much controversy.

The first ballot marking devices emerged in the late 19th century, but were only widely used in the last few decades. Today, electronic BMDs have come into widespread use as assistive devices in the context of optical scan voting systems to provide compliance with HAVA, though in recent years vendors have proposed that the devices be used by all voters.

ES&S AutoMARK

The AutoMARK is an optical scan ballot marker that is designed for use by voters who are unable to personally mark an optical scan ballot. The AutoMARK works in conjunction with an optical scanner. It was developed by Vogue Election Systems and the product line was purchased by ES&S. The machine features several features to enhance accessibility for voters with physical impairments or language barriers.

As of 2018, the AutoMARK was in use in 28 states.^

Optical Scanners

Optical scanners are digital scanning devices that tabulate paper ballots that have been marked by the voter. Ballots are either scanned at the precinct (in a precinct count system) or at a central location (in a central count system).

Diebold AccuVote OS

The AccuVote OS is an optical scan voting system. It can be used by precinct count systems and central count systems. Voters cast their ballots by inserting them into the AccuVote OS system, where votes are digitally tabulated, recorded, and stored. Originally marketed as the Unisys ES-2000, the machine later became known as the Global Election Systems AccuVote-OS Precinct Count (AVOS-PC) paper ballot scanner. In recent years, the machine has also been marketed and/or supported under the brands Diebold, Premier, ES&S, and Dominion.

As of 2018, the AccuVote OS was in use in 26 states.^

ES&S: M650

The M650 is an electronic ballot scanner and tabulator manufactured by ES&S. The ES&S M650 is used for counting both regular and absentee ballots. It launches ballots through an optical scanner to tally them, and keeps count on an internal 128 MB SanDisk Flash Storage card (pictured below). Election staff are responsible for configuring the M650 for each election.

As of 2018, the M650 was in use in 23 states.^

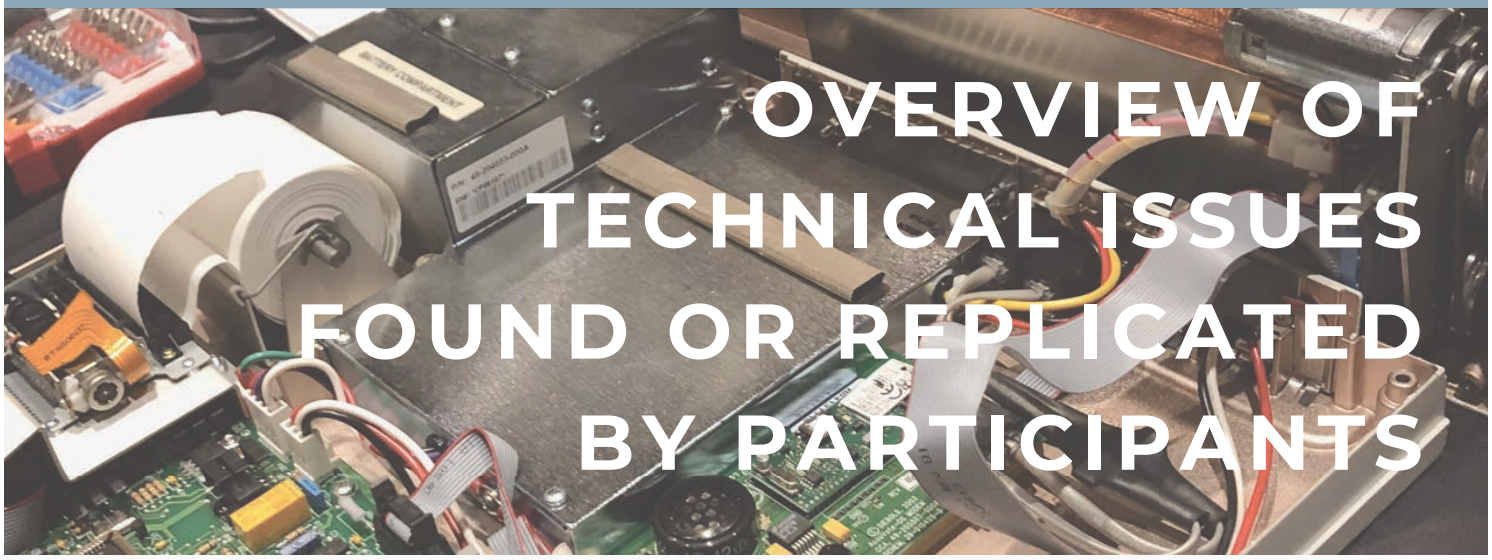
Hybrid Systems

Dominion: ImageCast Precinct

The Dominion ImageCast Precinct is an optical scanner paper integrated with DRE ballot marking device. It scans human-marked ballots, allows voters with disabilities and other voters requiring assistance to use the ballot-marking device to mark and review their ballots, and stores ballots for tabulation after the election period.

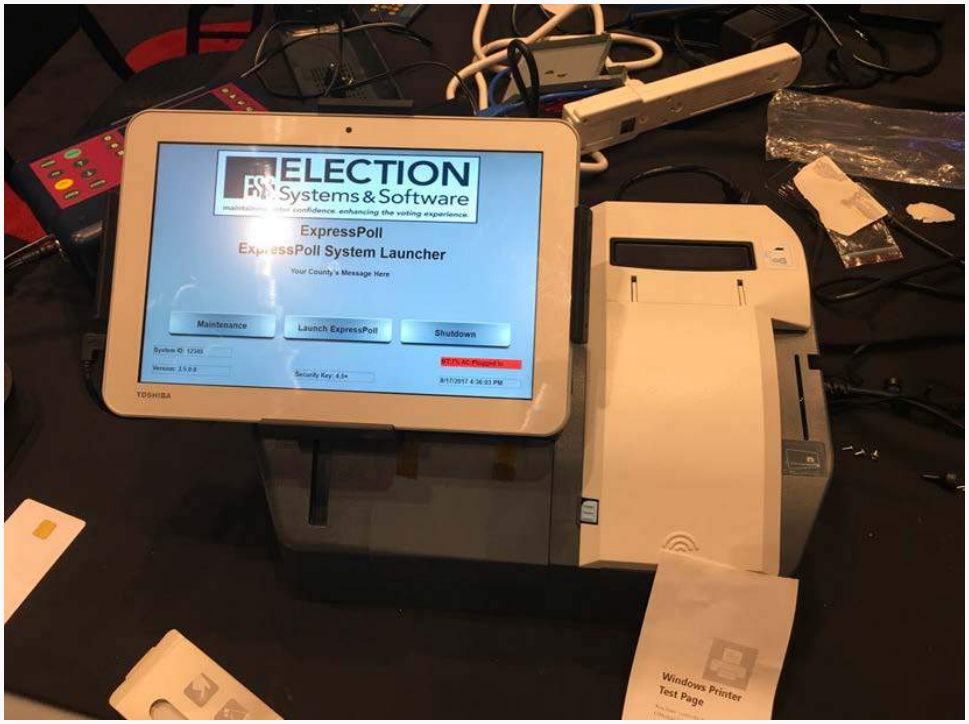
As of 2018, the ImageCast Precinct was in use in 10 states.^^

^ "Polling Place Equipment." The Verifier. Verified Voting. Accessed September 26, 2019. https://www.verifiedvoting.org/verifier/.
^^ According to survey of publicly available information conducted by DEF CON Voting Village.



OVERVIEW OF TECHNICAL ISSUES FOUND OR REPLICATED BY PARTICIPANTS

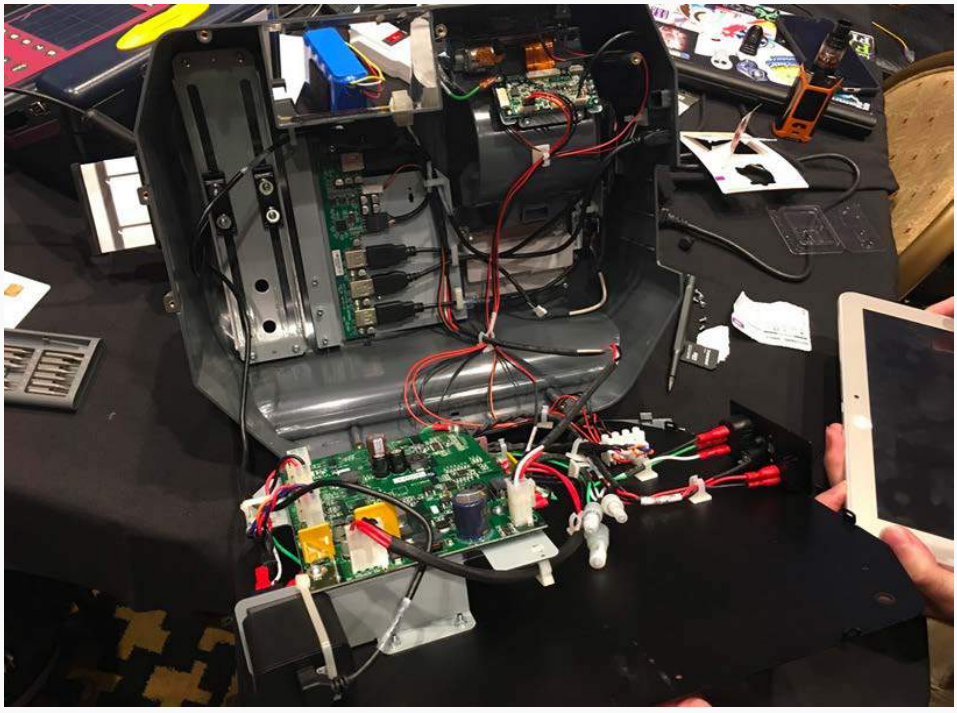
ES&S: ExpressPoll Tablet Electronic Pollbook



Picture: ES&S Electronic Pollbook System on an integrated stand with built-in printer, smart card reader, and other integrated peripheral devices.

The ES&S ExpressPoll Tablet Electronic Pollbook is an e-poll book which uses a standard commercial unencrypted Toshiba tablet held in place to a dock by a rubber locking mechanism. The specific model of the tablet was a Toshiba Encore 2 with Intel Atom CPU and running Windows 8.1 32-bit operating system.

The tablet can be popped out of its dock, exposing an SD port and a USB port of the tablet itself. Additionally, a USB hub is built into the mounting stand, which exposes additional USB ports. All these ports are active. The ports outside the mount are accessible to voters and poll workers without any physical locks or mechanical support for tamper-evident seals.



Picture: Internal electronics of the e-poll book stand. Internal USB hub visible is also directly connected to externally exposed USB connector. The researchers in the Village were able to print out with the voter permission slip directly by connecting into external USB.

While the SD card, which contains voter data, is encrypted, all keys are stored in plain text in a standard xml file allowing all data to be easily accessed and modified, thereby rendering encryption meaningless.

A card or USB device may be placed into the machine directly even when the dock is locked; the locking mechanism does not prevent access to the externally exposed ports on either on the tablet or on the stand.

None of the BIOS passwords were set. This allows unrestricted access to all system settings. By default, the device booted from a USB first without any password required.

The supervisor maintenance password is stored in plaintext on this device. In this case, the password for the tablet was “ESS”.

Security features supported by the underlying commercial hardware were turned off or not activated. The tablet supported Secureboot, a common security feature designed to check to see if the system has been tampered with and prevent the machine from running code of unknown origin. This was disabled by default on the tablet, allowing the e-poll book to load unsigned code from any source.

Picture: Externally exposed USB port on the side of the Electronic Pollbook Stand. The port does not get locked when the stand is locked and it does not have a lid or hook on which to place a seal.

As the Toshiba tablet is a standard off-the-shelf 'PC compatible' general-purpose device, it is supported by a wide range of general-purpose operating systems. This machine can be booted from a version of Linux using, for example, the external USB port and USB memory stick. Booting from Linux allows an attacker to access data on the device without encountering any Windows operating system-based defenses. Voting Village participants confirmed that an attacker would then be able to freely access data and run custom software, including software that would allow extraction of voter data. An attacker could also change or delete any voter registration data (like party registration) stored on the machine once the machine has been accessed.

The e-poll book operating system stack lacked any attempt to perform even the most rudimentary platform hardening. In fact, none of the bloatware that would come with a standard Toshiba tablet was removed. Apps for Netflix, Hulu, and Amazont were present in the e-poll book.

The lack of hardening is especially dangerous given that for one of the recommended deployments the system is intended to communicate over WiFi with wireless internet access to either Amazon Web Services or Microsoft Azure-based cloud services. Given that the operating system is unhardened and given that the standard bloatware provided by the vendor is present on the machine, there is an extremely wide, unprotectable, exposed attack surface.

ES&S AutoMARK

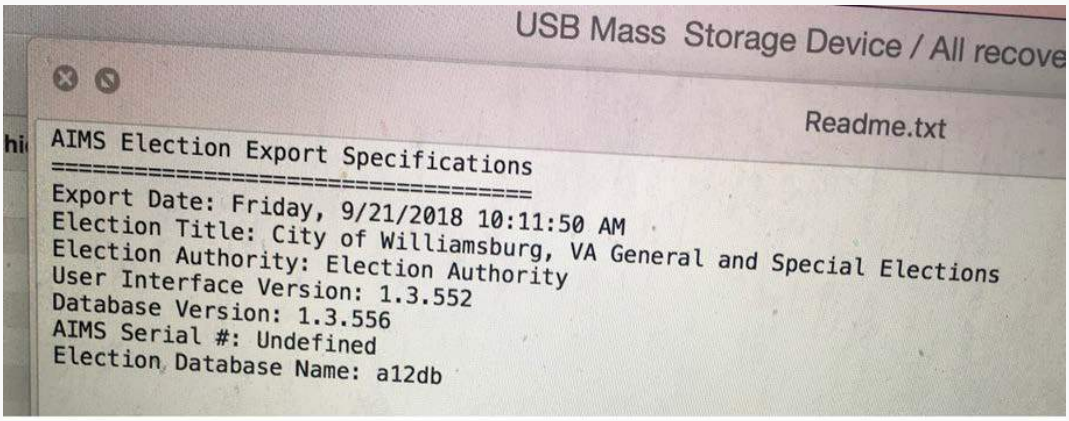
Picture: ES&S AutoMARK Ballot-Marking Device

The ES&S Automark is a ballot marking device that allows keyboard and ethernet ports to be plugged in after removing the top of the machine's case. The casing is closed only by 3 screws and does not include any tamper-evident seals. Immediate root access to the device was available simply by hitting the Windows key on the keyboard.

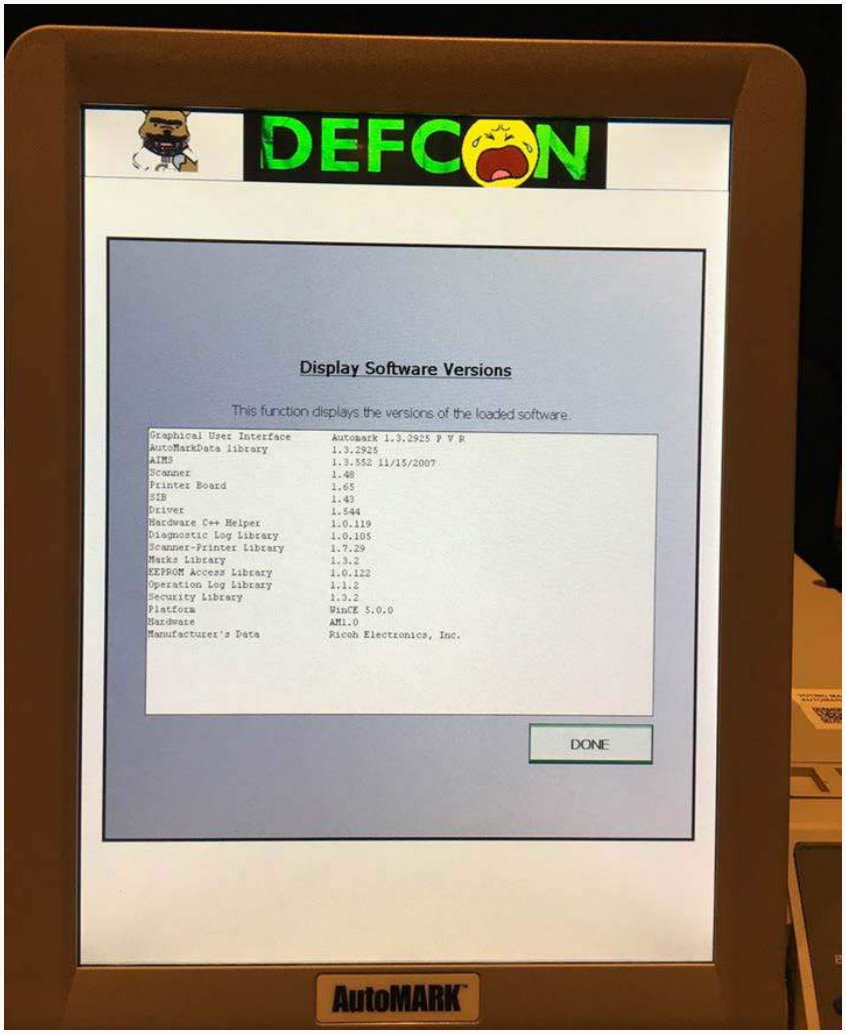
The lock to this device can be picked manually, allowing root and physical access to the unencrypted drive.

A RJ45 jack appears to be hidden behind a sticker on the front of the machine, accessible by removing the sticker without any tools.

The ES&S AutoMARK runs Windows CE Embedded Operating System 5.0. The application software in the machine appears to be last updated around the end of 2007, and the system appears to have been last used in a special election in late 2018.



Picture: Election database manifest file from the AutoMARK showing details of the last election for which it was used.



Picture: AutoMARK software version screen.

Operating system implementation has not been hardened or unneeded elements removed to minimize attacking surface. For example, Internet Explorer is present on this device.

Because the operating system is not hardened, an attacker can, before the machine boots up, drop malware onto the device after holding the “screen” button for five seconds.

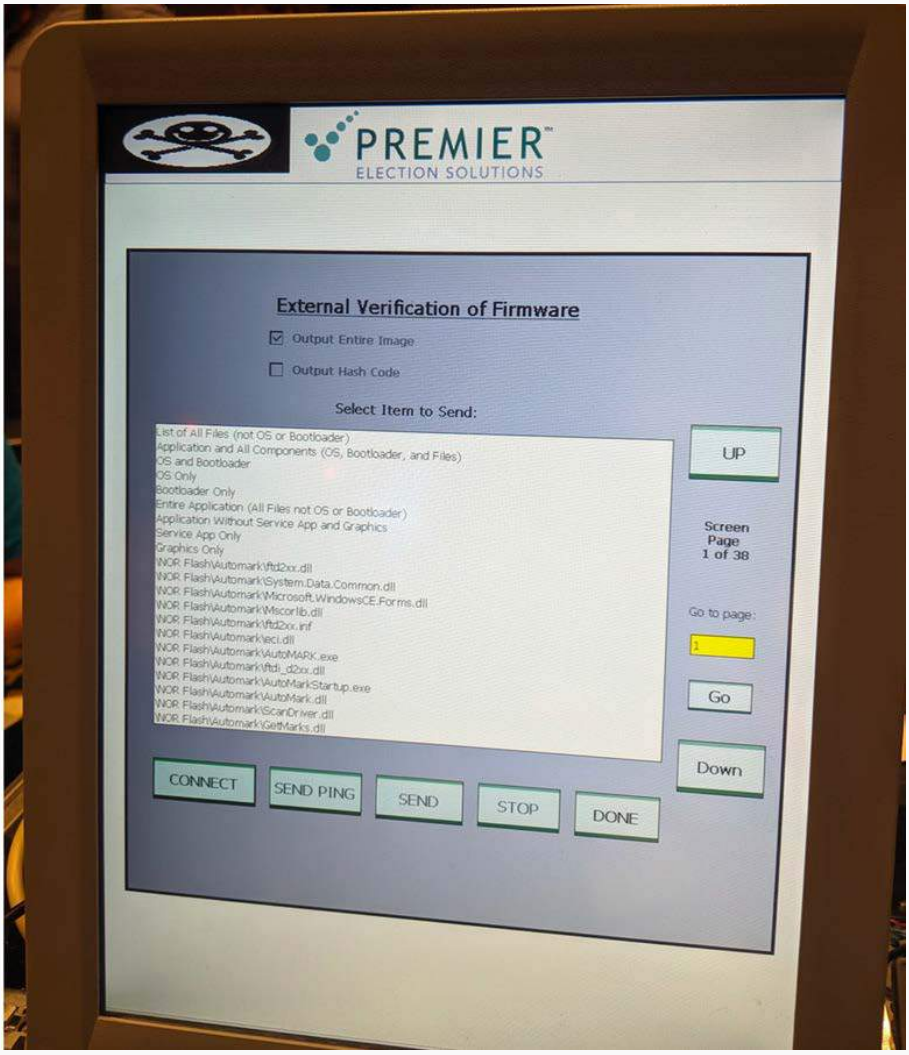
Collectively, a few people were able to change the group IDs of political parties still stored in the device from the previous election. However, this triggered a warning screen, indicating some form of integrity-checking for the stored data.

The embedded Windows operating system has special feature "Allow data connections on device when connected to PC" to enable Windows Mobile Device Center to allow the general purpose Windows version communicate with embedded windows. This feature was turned on.

The machine used several passwords/pins which were very simple, including passwords listed as default passwords in online manuals. These codes include “1111” as the pin code to replace the entire firmware of the device.

Participants were able to adjust the load address which caused the voting applications software to consistently crash. In this instance, the reason for the machine crashing would not be obvious to nontechnical people, such as the volunteers helping to run the polls, thereby creating an effective denial of service attack which would be hard to remotely diagnose.

Additionally, the administrator password was stored in the clear in the configuration file and participants were able to use it to enter admin mode. This enabled them to look at the binaries and replace the header on the voting machine with one of their choosing. Nick Bishop was one of the participants responsible for these discoveries, and has willingly identified himself.



Picture: AutoMARK firmware function enabling automated extraction of the whole system image.

Participants managed to place the DEF CON logo in the header portion of the screen and were able to edit the registry. Using a screwdriver to open up the machine, participants were able to plug a keyboard into an exposed USB port and operate the voting machine as a standard Windows CE machine after exiting the specialized voting software.

Participants Minoo Hamilton and William Baggett also discovered the default system maintenance password by searching on Google, revealing “admin” as the identification name and “vogue” as the password. This allowed both of them to gain access to the securities section on the machine, enabling them to make changes and access vital information. From the securities section they were able to run a remote integrity check that displayed the files and the integrity of each file. Mr. Baggett discussed potential implications for these risks for issues involving a forensic change of evidence. Depending on the protocol adopted by an election office, it is possible that if an attacker modified the access database or central tabulator after hacking their way in, the integrity of the modified data would not be checked against the centralized system.

Dominion Imagecast Precinct

Picture: Dominion ImageCast Precinct with Ballot-Marking Device screen turned to face the scanner (back) side of the machine.

The Dominion ImageCast Precinct is an integrated hybrid voting equipment. It combines an optical paper ballot scanner and ballot marking device and allows for nonvisual accessibility for the blind and visually impaired, in compliance with HAVA. This machine provides voters with disabilities the same opportunities for access and participation as other voters.

This device integrates the devices and the ballot box to store the cast ballots into one unit, but has a single locking mechanism that holds the entire ballot box together. If picked, ballots could easily be stolen using common items such as a standard trash picker.

Participants were able to access USB, RJ45, and CF slots on this machine without using destructive force.

The system also runs Busybox Linux 1.7.4, which has twenty currently known medium to high level vulnerabilities including the ability to allow remote attackers to allow a DNS through CPU/bandwidth consumption via a forged NTP packet which triggers a communication loop with the effect of Denial-of-Service attacks.*

* Search Results. Common Vulnerabilities and Exposures. Accessed September 26, 2019. https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=busybox.

Boot settings also allow for the system to be booted from an external USB on startup.

Importantly, the CF card and card readers on the front and back of the machine are physically exposed, and could be replaced.

Additionally there is an internal USB port that is not exposed and an external CF slot that is covered by a tiny door. Either slot can be used to load the OS. Boot order is USB then CF.

The door opens by unscrewing one of the screws. The screws in question were so-called secure screws. Participants made a quick run to a nearby electronics store to purchase "Security Bits Set with Ratchet Driver" for under $28 which was used to open all 'security screws' used in any of the machines.

Picture: Small unmarked lid on the side of the machine for accessing CF card slot inside of the machine. So-called "secure screw" tips can be commonly purchased from any electronic store.

When participants removed the CF card on the front of the machine, they found scanned ballots and the configuration file in the clear. In the absence of other protections, modifying configuration data could allow an attacker to edit which X/Y locations on the scanned ballots matched with which candidate. Participants found no digital signing or encryption protecting those digital files.

Participants responsible for much of the work on this machine identified themselves willingly: Zander Work, Lyell Read, Cody Holiday, Andrew Quach, Steven Crane, Henry Meng, and Nakul Bajaj. As a group, they were able to boot an operating system of their choice and play video games on the voting machine, including a popular game called "Pong". These participants averred that by bringing a simple screwdriver and CF card into the voting area, an attacker could use a screwdriver to access the machine's intended CF card and swap it with the card they brought, allowing the attacker to boot an arbitrary operating system and take control over the machine.

The group was able to browse the file system on the CF card, proving that the filesystem was unencrypted and unprotected.

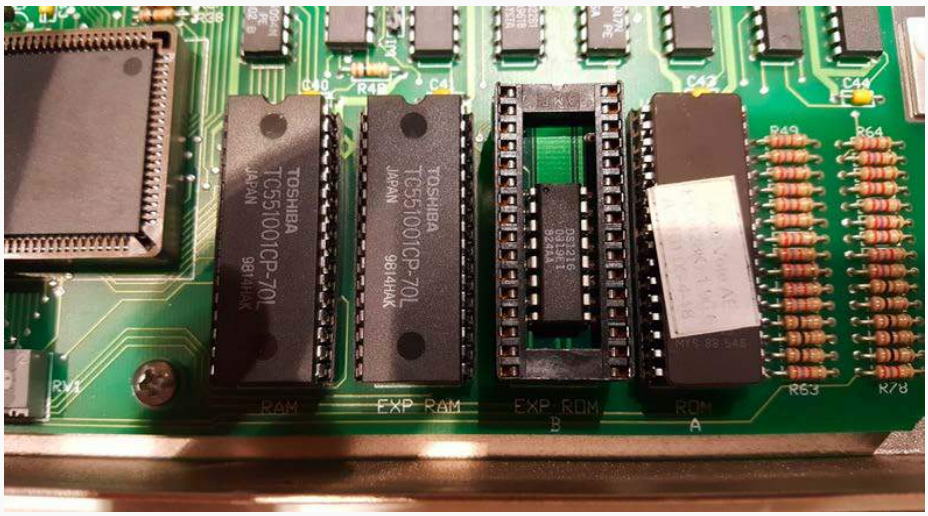
AccuVote-OS Precinct Count

Picture: Originally marketed as Unisys ES-2000 later become Global Election Systems AccuVote-OS Precinct Count (AVOS-PC) paper ballot scanner. Later also marketed/supported under brands Diebold, Premier, ES&S and Dominion.

Participants also discovered a set of previously undocumented functions in the Dominion/Diebold/Premier/ES&S AccuVote, enabling remote manipulation of the machine's memory card when the machine is connected to a network — without any physical access to the memory card, and without breaking or circumventing any physical seals. Researchers confirmed the existence of these features with a person who has previously been involved with the maintenance of these machines, and an election official who had encountered the feature before. The investigation of these functions and possible mitigations is ongoing at the time of this report.

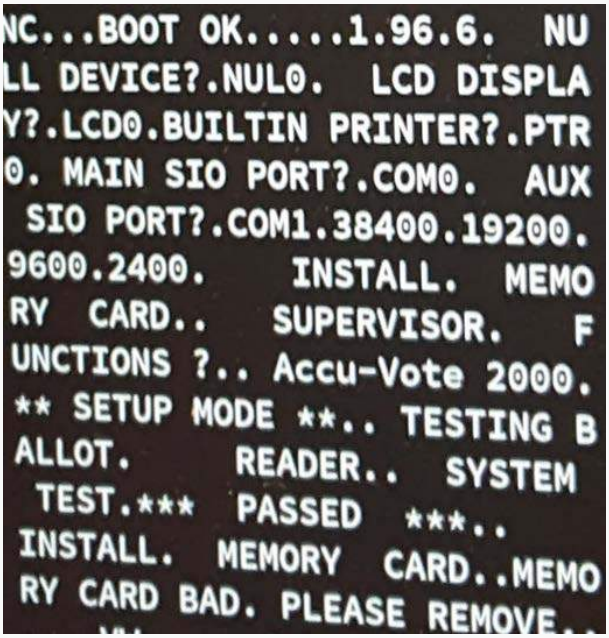
The Voting Village acquired two dozen devices from the same jurisdiction. From the circumstantial evidence of documents in the travel cases, it appears that the machines were put in use and subsequently retired together. However, the devices did not have the same software version installed. Despite possibly having been used in the same elections, some of the machines had software version 1.96.6, whereas others were running 1.96.4, an older version.

In this device, the software is installed on a socketed EPROM microchip. EPROM stands for Erasable Programmable Read-Only Memory and it is a type of programmable read-only memory (programmable ROM) that can be erased and reused. This type of chip has to be physically removed from the circuit board, placed into a separate programmer device, and completely erased before it can be reprogrammed. Erasing the chip is done by shining an intense ultraviolet light through a window through which the silicon chip is visible. The erasing window must be kept covered with an opaque label to prevent accidental partial or unstable erasure by the UV by sunlight or camera flashes and therefore the window is always covered by a sticker as seen in the picture.



Picture: AVOS circuit board with socketed EPROM chip containing election software. Software upgrades to this machine are installed by physically replacing the chip; as the chip is socketed, this can be done in a matter of seconds. The chip inside a socket is a SmartWatch CMOS real time clock with an NVRAM controller circuit and an embedded lithium energy source.

This machine was originally developed in 1986 and first introduced to market in 1989, and it is believed to have been used for the first time in U.S. general elections in Minnesota in 1990. The CPU of the system is NEC V25, which was the microcontroller version of the NEC V20 processor. The V20 was a processor made by NEC that was a reverse-engineered, pin-compatible version of the Intel 8088 with an instruction set compatible with the Intel 80186. It has 16-bit internal architecture and 8-bit external data bus. The V20 was introduced in 1982 and V25 was officially phased out in early 2003. The EPROM containing the programming was 128KBytes in size and the system had two RAM chips 128KBytes each.



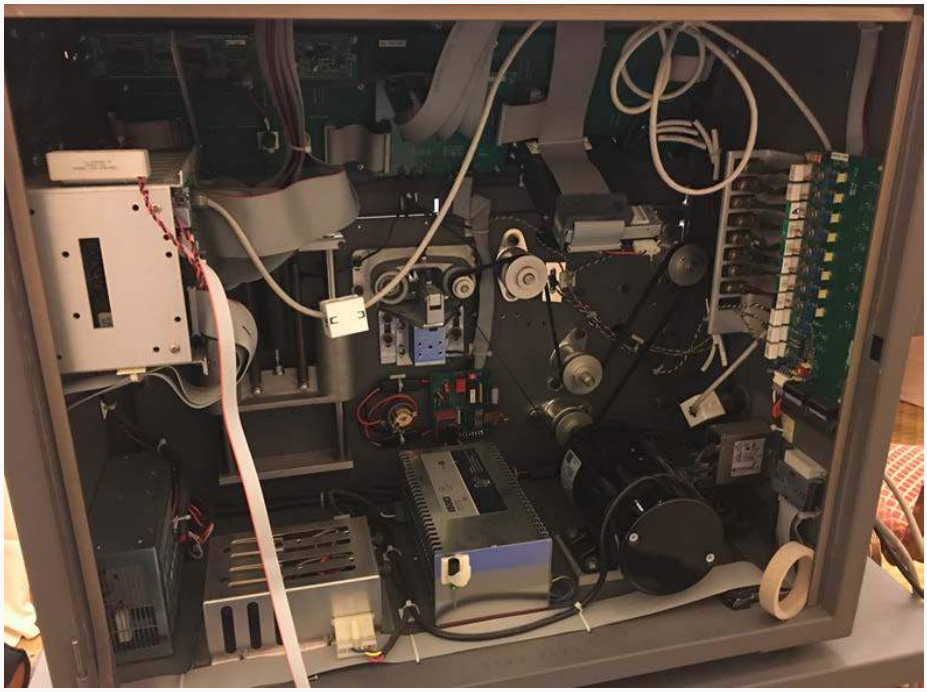
Picture: Human readable strings from the chip contained in the programming. As is typical for embedded systems of the era, the programming contains a lot of clear text strings. In this era of technology, compression and encryption were things of the future.

EVID

Picture: VR System EViD electronic poll book system.

Participants confirmed that the hardware for this machine is a normal general purpose PC hardware which is very low-end by today's standards. There was no BIOS password set on the machine. Consequently, participants were able to boot an arbitrary operating system off a live CD, which had the ability to run on 32-bit and limited to 128M RAM. Ultimately, the device was used as an entertainment device, amusing visitors with Nyan Cat.

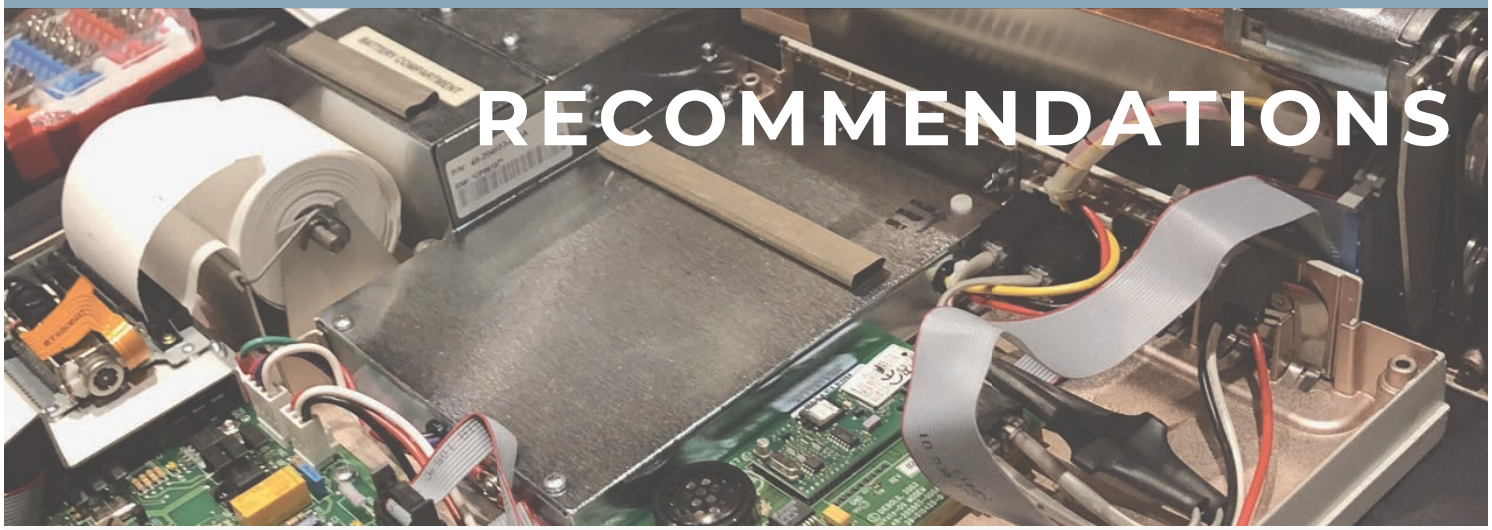
ES&S M650



Picture: Inside of ES&S M650 Optical Paper Ballot scanner. Storage devices and other electronics are quick and easy to replace in a card rack in the upper left. Note the overpowered for the purpose electric motor for moving the paper ballots.

Last year, the Village made accessible to participants two M650 units which had been used in Oregon. This year, the Voting VIllage acquired an additional unit used in the state of Washington. Based on documentation, all three devices were from the same year and same hardware revision. Based on that, the researchers were surprised to discover that the hardware and the features between the devices were not identical. It is unclear who had carried out the modifications.

The paper maintenance log inside the machine did not answer that question, but showed that maintenance personnel periodically have physical access to the inside of the machine. With physical access, this type of machine has no security protections against any kind of modifications.



RECOMMENDATIONS

While the DEF CON Voting Village is heavily focused on the technical aspects of the election infrastructure, the Unhack the Ballot initiative underlined the importance of all levels of the human factor aspects in an election ecosystem. Election officials need more training and better access to parties who can help them to navigate the consequences of technological choices around them. Bearing in mind that at the moment many of those choices take place in the long out-sourcing supply chains of the ecosystem and election officials are left into the tail-end of the process to design mitigation strategies into deployments which they were not participating in design. Election officials also need help to train their own staff to be more security-minded and to gain the 'muscle memory' instincts to protect day-to-day operations, both during election cycles and between them.

The security implications of ballot marking devices should be further studied. This calls for multi-disciplined research looking into the various aspects of the election process from integrity and security to usability and reliability. Current and proposed next-generation ballot marking devices have not been designed with security considerations in mind. They open the door for various methods to attack the election process. In the simplest end are denial-of-service attacks and attacks to compromise the secrecy of the ballot. Depending on the deployment strategy, the ballot-marking device will know a lot about the voter and therefore ballot-marking devices can be hacked specifically to, for example, disenfranchise vulnerable populations: voters who use audio interface, sip-and-puff, large fonts, non-English language ballots, or who take a long time to vote. The discussion about 'detecting' hacked devices is dangerous, because in the absence of remedies even if irregularities are reported there is almost no way to properly investigate. Ballot-marking devices as currently deployed have an insurmountable security design and delegation flaw: the protocols make voters responsible for checking whether devices are performing correctly, and voters cannot get any evidence to prove to others that a malfunction occurred and therefore even if voter detects and reports an error, it would often be the only remaining course of action for poll workers to assume a mistake on the voter's part.

The use of barcodes should be carefully analyzed from various security aspects. Malicious fraudulent advanced barcodes have been causing a lot of problems to Point-of-Sale systems and utilizing bar codes in elections opens a new avenue for injection and scripting type of attacks. The

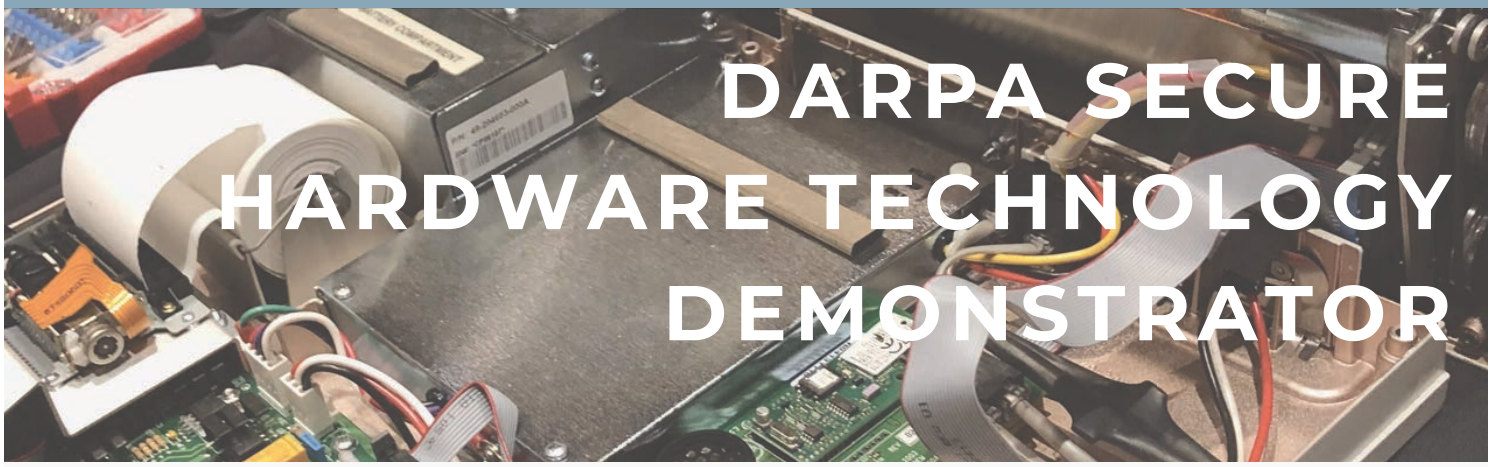
election integrity, auditability and transparency aspects of using barcodes are even more important. Paper ballots have been promoted because they make those various methods of audits possible. This is true only if the significant record of the vote is human readable. At this point in time, we have to recognize that there are two aspects: technological soundness and the public trust. In elections, it is important that the losing parties and their supporters accept the results as fair. Any method of voting which is not completely transparent and understandable by everyone can be contested in the court of public opinion.

Hybrid machines, which offer users the option of inspecting their ballot before printing, should be avoided because they increase the risk of undetectable attacks. Because the machine knows which ballots are inspected and which are not, it can modify only those that are not inspected — essentially undermining the purpose of voter-verifiable ballots. Such attacks would be very hard to detect exactly because the attacked ballots are those not inspected. With today's razor-thin margins of victory in elections, even the ability to modify a small percentage of the votes undetectably can have a huge impact.

Inspection of newer models of e-poll books further underlines the absence of security design both in software, hardware and physical security aspects. E-poll books are inherently networked devices to synchronize across all devices at a polling place and to avoid cabling, which is often done wirelessly. Furthermore, many new makes and models of the e-poll books actively communicate in real-time over the Internet to back-end servers hosted in commodity cloud services. So far, the e-poll books studied in the Voting Village have been utilizing general-purpose operating systems on commercial off-the-shelf hardware with no special hardening or security measures.

Historically, security measures provided by the hardware / low-level programming have been systematically turned off in all classes of devices used as part of the election infrastructure. Unfortunately, this was found to be true also with newer generations of voting equipment in the Village. These practices greatly simplify paths to attack the machines and also place increased to unbearable burdens to physical security and chain-of-custody management of the machines over the entire lifetime of the devices.

Election reporting was increasingly an area of concern in the Village discussions. With the election night beginning of the process happening over the internet as well as the end of the process as reporting happening over the Internet, discussions in the Village were drawn into similar information flow designs in other industries and how irregularities in those setting had managed to go unnoticed when the ends of the process are seemingly matching. There needs to be a process in place to verify that the reporting truly is sum-of-its-parts.

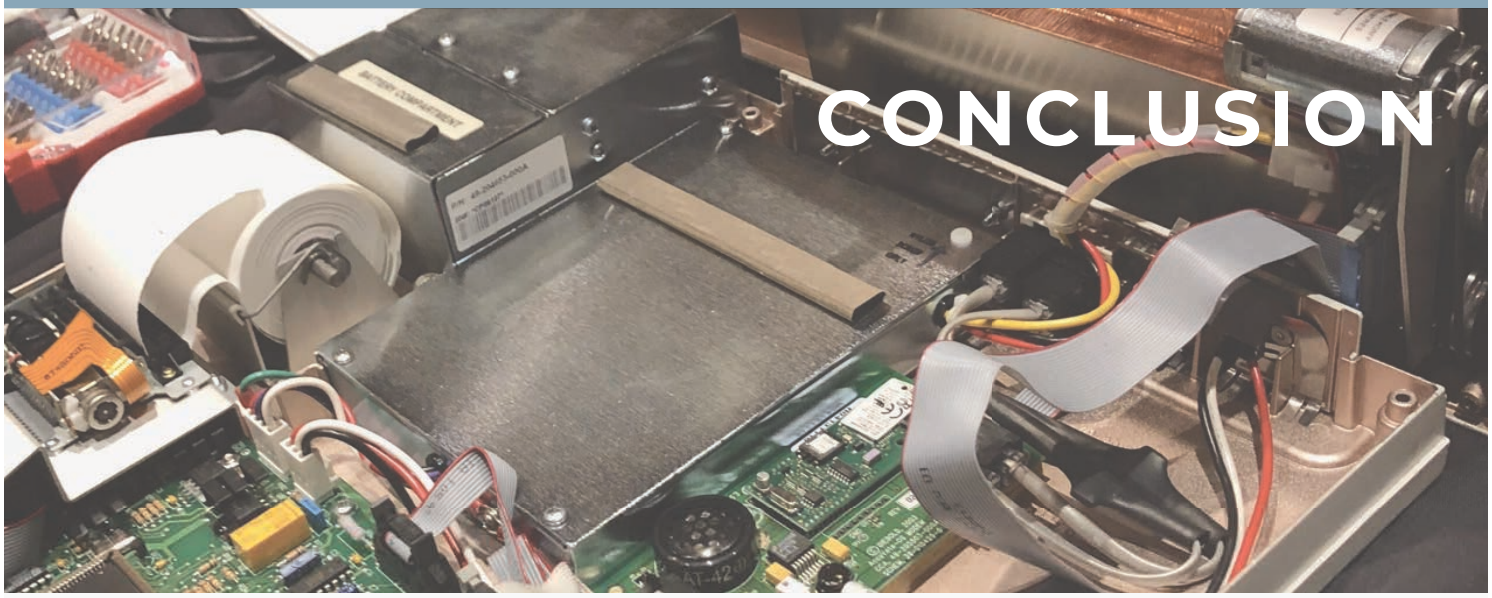


DARPA SECURE HARDWARE TECHNOLOGY DEMONSTRATOR

Since December 2017, DARPA has been working to build next-generation secure hardware through its System Security Integrated Through Hardware and Firmware (SSITH) program. This new hardware was unveiled for the first time to the public in the Voting Village.

The SSITH program develops methodologies and designs tools that enable the use of hardware advances to protect systems against software exploitation of hardware vulnerabilities. To evaluate progress on the program, DARPA has incorporated the secure processors researchers are developing into a very early prototype application of a secure voting ballot box. At the Voting Village this year, they turned the system loose for public review by thousands of hackers and DEF CON community members. The purpose of this application is solely to provide a demonstration system that facilitates open challenges. To be clear, the SSITH program will not produce a voting system, nor will it provide a specific solution to election system security issues for use during elections.

During DEF CON 2019, the SSITH system demonstrator consisted of a set of RISC-V processors that the research teams will modify to include their SSITH security features. Since SSITH's research is still in the early stages, only one prototype version of the 15 processors in development was available for evaluation. DEFCON 27 was the first small step on a path to evaluate the hardware design. In 2020, DARPA plans to return to DEF CON with an entire demonstrator system, which will incorporate fixes to the issues discovered during this year's evaluation efforts.



CONCLUSION

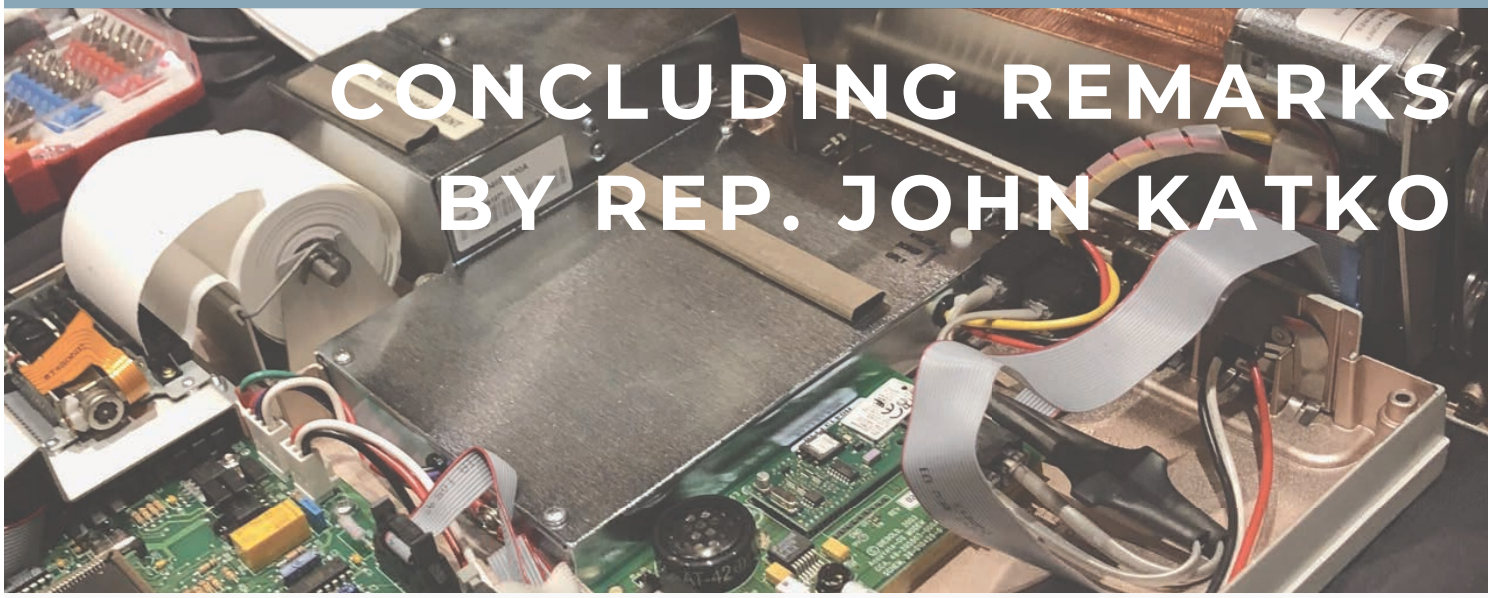
As in previous years, this year's Voting Village demonstrated vulnerabilities inherent in the election environment and highlighted the enormity of the task of securing our nation's elections. Among the many issues highlighted at the Voting Village this year, particularly on machines previously unavailable to the hacker community, three serious vulnerabilities stood out:

1. Widespread use of current ballot-marking device architectures poses new systemic security risks
2. Previously studied commercial election equipment continues to surprise with new weaknesses
3. Many systems are shipped with basic security features disabled

If we as a nation are serious, as we must be, about improving election security in the United States, particularly ahead of the 2020 presidential election, the Voting Village recommends that the following as urgent priorities:

I. Nationwide deployment of mandatory post-election risk-limiting audits
II. Nationwide deployment of voter-marked paper ballot systems
III. Dramatically increased funding and other resources to help local election officials protect their IT infrastructure from foreign state actors and other threats.

Without taking these steps to support election administrators at the frontlines of this clear national security threat, we fear that the 2020 presidential elections will realize the worst fears only hinted at during the 2016 elections: insecure, attacked, and ultimately distrusted.



CONCLUDING REMARKS BY REP. JOHN KATKO

The following is a transcript from Representative John Katko's remarks at the Voting Village Report release on September 26, 2019.

Good afternoon, everybody. Oh wake up, come on, I know it's not bad. Good afternoon. *[Audience responds: Good afternoon]*

Thank you for being here and, I never thought I would be saying this, I know the media is here and some others, but for those of you who are hackers, I guess I say 'welcome.' And I know there's a few here and you definitely serve an important part of this endeavor we're trying to work on.

I want to thank Congresswoman Speier for inviting me to speak, I really appreciate that, so thank you, Jackie.

I want to thank Matt Blaze for helping start the Voting Village and for discussing election security with me last week. We had a great discussion.

You know, as chair of the - or ranking member of the Homeland Security Cyber subcommittee you are trying to keep up with the pace of the bad guys and you are trying to keep up with the pace of our vulnerabilities. And that is a very daunting task.

It's clear from my discussion with Matt, it's clear from my time on the subcommittee, that it is, this is probably the number one threat to our country right now, is our cyber vulnerabilities.

And everything from cyber hygiene to offensive cyber capabilities if necessary, has to be discussed and has to be examined.

Election - elections are at the, strike at the fundamental heart of our democratic system. Elections are what we, we as a people founded our democracy upon. And it's clear that the bad guys are trying to hit our elections.

So, some things I figured out by talking to Matt and talking to many others, that are fundamentally clear to me: we are not gonna be able to do a system that is 100% fool proof no matter what we do. And that's a sobering reminder of the vulnerabilities, but we have to accept that.

So what do we do?

There's really kind of three pillars that I see, that we can do.

Is, number one, the voting machines themselves. And, number two, is the infrastructure that surrounds the voting machines, within it, like board of elections in New York State, for example.

And then what can we do to probe the systems to make sure they're good, and that's called risk limiting audits.

So, the voting machines themselves. After the 2000 debacle, the hanging chads and everything, we kind of tended to drift away from paper ballots, but now they're back. And they're back for a reason. Because we have to have a paper back-up to the electronic voting mechanisms that we have, just in case there's, something happens. I think it's critically important.

In New York state where I am it took 'em forever to get to that change but now we have a, a very good system where you fill out a sheet of paper and they scan it into the machine. And I remember it well because when I first ran for reelection I filled my ballot out wrong. I had to be reminded with the cameras all there that I filled my ballot out wrong.

So, maybe I was nervous, I don't know, but we have that now. It's not everywhere across this country, so we have to have those stand alone machines Those machines cannot be connected to the internet. They have to be stand alone machines.

Then you talk about the infrastructure around that. You talk about the board of elections, you talk about how they get the information from the machine and then tabulate all the votes. How do you do that? And how do you make sure you don't affect those machines themselves.

I think that's very important. That's going to take money. A lot of these states and municipalities, they have terrible decisions to make. Do we fix the potholes, or do we fix our election machines? And what's more tangible looking to them?

So it's hard and I think there's a role the government can play in providing that funding. And we need to do that.

And then the third thing is, and perhaps, I think, the most important thing, that Matt and Harri told me, and others, is doing the risk based auditing, if you will. And taking the machines even though you don't know there's anything wrong, go back over every once and a while and make sure by spot checks, I'll just give some background, in spot checking they have a hand recount,

retabulate - make sure that what's being reported is actually accurate. And that takes money, too. Those are the things, I think, the roles the federal government can play in election security.

And obviously getting the counties the best practices, but also getting them the money, so they can get the right machines, get the right security procedures in place, and get the right risk-limiting auditing procedures in place.

Those are the three biggest things that I see and everything that Matt's been doing here with the Voting Village and the DEF CON, all that stuff's really important because it helps us expose the vulnerabilities. We can never ever let our guard down, but if we can do those three things that I articulated and, believe me, I have other ideas but I am not going to articulate them here, that will go a long way toward it.

So whatever legislation that we come up with, it should most definitely deal with all three of those things. And anything I can do to help that, the Congresswoman or others, I would absolutely do.

And as always, I need input from you. Matt knows I listen to him and I will listen to others because you know I by far am not the expert on this.

One thing I have learned in homeland security is, as we get our defenses better, the bad guys get their offensive capabilities in that much more in tune.

I'll tell you because when I started out it took much more than something like this to take out an airplane and now this is all you need. *[holding up cell phone]*

So the bad guys are trying to perfect bombs, they're trying to perfect offensive terrorist capabilities, and they're trying to perfect offensive cyber terrorism capabilities. We have to be - never let our guard down. So that's why what you're doing here is so important.

We appreciate it very much and I'll just close with, get the information to us. Please, if you have ideas, no idea is outlandish. The only idea that is a bad idea is one I don't hear about. We can sift through what we think is good.

But the pillars that I think of are the stand alone machines, spot checking them, and having good infrastructure around them and good people around them is critically important and we can play a role in that.

So with that I'll say thank you very much and God bless. Have a good afternoon.

AFTERWORD
BY REP. JACKIE SPEIER

In 2016, we faced an unprecedented attack on our election by the Russian government, with criminal interference and disinformation poisoning our public discourse. Fortunately, the nuts-and-bolts administration of the election, from registering voters to tallying their ballots, was not, as far as we know, demonstrably affected.

This was not for lack of effort, however, and we must not breathe a sigh of relief.

I felt fear in my heart when I heard Special Counsel Mueller, testifying before me and the House Intelligence Committee in July, state without any equivocation:

"It wasn't a single attempt, they're doing it as we sit here, and they expect to do it during the next campaign. … Many more countries are developing capabilities to replicate what the Russians have done."

To my question about the ultimate takeaway, Special Counsel Mueller told us to focus on "that aspect of [his] investigation that would have long-term damage to the United States that we need to move quickly to address," and that his report was a "living message . . . for those of us who have some responsibility."

As citizens, we all bear this responsibility. The call to action has been answered by the grassroots efforts of the Voting Village and the patriotic hackers that have dedicated their talents to improving our election infrastructure. It is time for Congress to answer that call as well.

Former FBI Director Mueller's alarm joined a chorus of alarms that have been blaring loudly about the security of our elections for over three years. Just recently, the Senate Committee on Intelligence released a redacted report that found that "[t]he Russian government directed extensive activity . . . against U.S. election infrastructure."

In response to this terrifying threat, the House of Representatives passed two landmark bills that would guard our elections from malevolent interference. H.R. 1, the For the People Act, would harden our election security by enhancing federal support for the most secure voting systems, such as paper ballots, increase oversight over vendors, and develop a national strategy to protect democracy. H.R. 2722, the Securing America's Federal Elections (SAFE) Act, would provide financial support and enhanced security for election infrastructure, including $600 million for paper ballots and paper auditing systems and a commitment to future funding for election infrastructure.

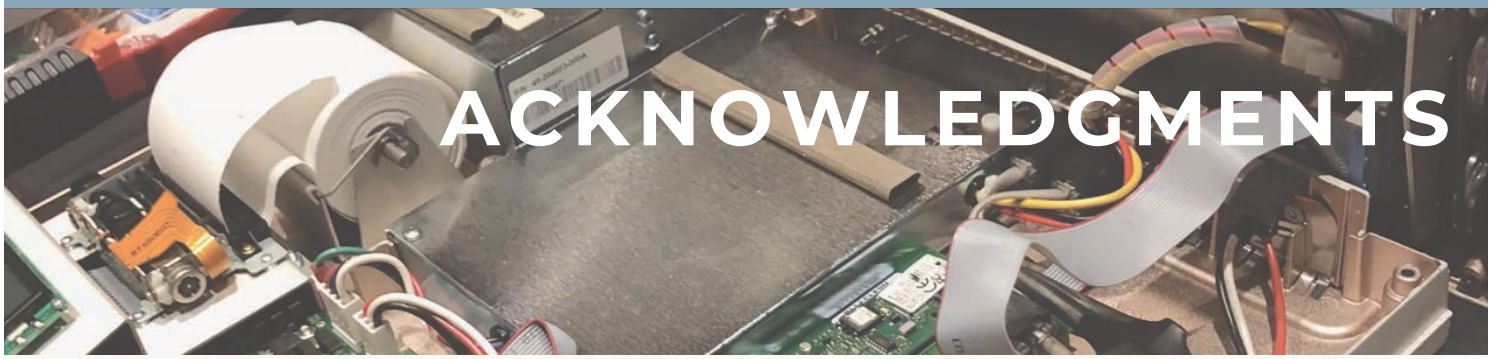
Yet Republicans in the Senate and this Administration have not taken up these crucial House bills or done much of anything to address this ongoing threat. Instead, they seek to undermine our intelligence communities and any efforts to fortify our election security. One has to ask oneself why that is—what could they possibly gain?

Having represented Silicon Valley for decades, I appreciate that the spirit of exploration and innovation, which can be used to disrupt and interfere, can also lead to a more vibrant and resilient society.

I believe that American ingenuity is up to the task of addressing the enormity of the problems we face. There are many vulnerabilities from a voter's registration to the tally. Voter rolls that are used to verify voters' identities as they enter the polls could be manipulated. The apparent technological ease of direct-recorded, entry touchscreen systems has been warmly embraced by many. But these systems also open up new avenues for interference.

Vulnerabilities in election systems strike not only at the infrastructure itself. Public awareness of these vulnerabilities also undermines confidence in elections and erodes trust in our system of government. Elections are the core of citizen participation, and when people feel their voice is silenced, increased apathy threatens to hollow out our government. It is a nightmare scenario – our votes – a sacred right which women and people of color in particular have had to fight and even die for – could be stolen from us. This is not an esoteric issue of ones and zeros, this is the frontline in what makes us Americans.

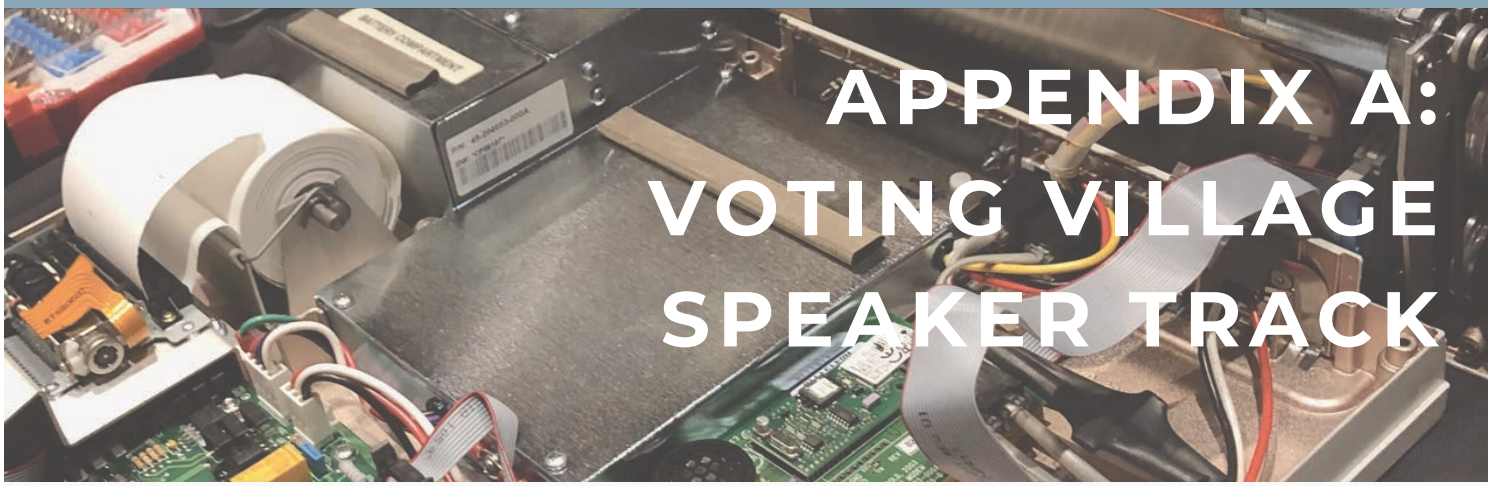
Voting Village's engagement with Congress has been a bright spot in the twilight zone of inactive agitation that typifies Capitol Hill. I urge my colleagues to join me and embrace engagement with election officials, security experts, and our patriot citizens who have answered the call to action for the benefit of us all.



ACKNOWLEDGMENTS

A number of individuals contributed to the success of the DEF CON Voting VIllage and the production of this report. A special thanks to:

- The organizers, subject matter experts, and partners who collaborated to make the Voting Village concept a reality and helped to author this report;
- The speakers and moderators of the Voting Village speaker track, including Senator Wyden, Representative Eric Swalwell, representatives of the U.S. Department of Homeland Security, the Defense Advanced Research Projects Agency (DARPA), and many others;
- The state and local election administrators who attended the Voting Village to share their wealth of experience and learn from the hacker community about the latest election system security concerns;
- The outstanding support and contributions of Jake Braun, Phil Stupak, Morgan Ryan, Jaclyn Houser, Analiese Wagner, Casey Dolen, Claire Martin, and Caroline Hymel;
- The indispensable legal advice and guidance provided by Kendra Albert, Sunoo Park, and Thomas Hopkins of the Cyberlaw Clinic at the Berkman Klein Center for Internet & Society, Harvard Law School; and
- Verified Voting and the Michael and Paula Rantz Foundation, for their generous support of this work.



APPENDIX A: VOTING VILLAGE SPEAKER TRACK

This year's Voting Village speaker track spanned all three days of the conference and featured members of Congress, representatives from the Department of Homeland Security and the Department of Defense, private sector pioneers, academics, researchers, and hackers of all stripes. Below is an overview of each day's talks, as well as each speaker's biographical information.

Friday, August 9, 2019

Welcome and Voting Village Kick-off Remarks

- **Harri Hursti, *Co-Founder, DEF CON Voting Village; Founding Partner, Nordic Innovation Labs***

  Harri Hursti is among the world's leading authority in data and election voting security, critical infrastructure, and network security systems. Beginning his career as one of the minds behind the first commercial, public email and online forum system in Scandinavia, he went on to cofound EUnet-Finland. Hursti has authored many studies on election security and vulnerability in both academic and corporate publications. He worked for Black Box Voting where he performed voting machine hacking tests, which became known as the Hursti Hacks. These tests were filmed and later turned into the acclaimed HBO documentary Hacking Democracy.

- **Matt Blaze, *Co-Founder, DEF CON Voting Village; Professor of Law and McDevitt Chair for the Department of Computer Science, Georgetown University***

  Matt Blaze holds the McDevitt Chair of Computer Science and Law at Georgetown University. His research focuses on the architecture and design of secure systems based on cryptographic techniques, analysis of secure systems against practical attack models, and on the intersection of computing and communication technology and public policy. In addition to his position at Georgetown University, he sits on the board of directors of the Tor Project. Blaze received his PhD in Computer Science from Princeton University.

- **Jake Braun, *Co-Founder, DEF CON Voting Village; Executive Director, University of Chicago Harris Cyber Policy Initiative***

  Jake Braun serves as the Executive Director for the University of Chicago Harris School of Public Policy's Cyber Policy Initiative where he works at the center of politics, technology and national

security to advance the field of cyber policy. Prior to joining CPI, Braun was appointed White House Liaison to the Department of Homeland Security (DHS) by President Obama where he was instrumental in the passage of the unprecedented Passenger Name Record (PNR) Agreement, one of the largest big data agreements in history. In addition, he worked on the development and implementation of the Homeland Security Advisory Council's Task Force on CyberSkills. Braun is also a fellow at the Council on CyberSecurity and is a strategic advisor to DHS and the Pentagon on cybersecurity.

Remarks by CISA Director Chris Krebs

- **Christopher Krebs, *Director, Department of Homeland Security's Cybersecurity and Infrastructure Security Agency***
  Christopher Krebs serves as the first director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Mr. Krebs joined DHS in March 2017, first serving as Senior Counselor to the Secretary, where he advised DHS leadership on a range of cybersecurity, critical infrastructure, and national resilience issues. Prior to coming to DHS, he was a member of Microsoft's U.S. Government Affairs team as the Director for Cybersecurity Policy, where he led Microsoft's U.S. policy work on cybersecurity and technology issues.

DARPA SSITH Program at DEF CON

- **Linton Salmon, *Program Manager, Defense Advanced Research Projects Agency (DARPA)***
  Dr. Linton Salmon joined the Defense Advanced Research Projects Agency as a program manager in September 2014. Prior to joining DARPA, Dr. Salmon spent 15 years in executive roles directing development of CMOS technology at GlobalFoundries, Texas Instruments and Advanced Micro Devices. Before joining Advanced Micro Devices, Dr. Salmon was vice president for Research and Technology Transfer at Case Western Reserve University and an associate professor of electrical engineering and physics at Brigham Young University (BYU), where his research areas included CMOS processes, micro-battery research, packaging and MEMS.

What Role Can Journalists Play in Securing Elections?

- **Maggie MacAlpine *(moderator), Co-Founder, Nordic Innovation Labs***
  Margaret MacAlpine is an election auditing specialist and system testing technologist. She has worked on a variety of projects that include electronic testing of voting registration systems, election security and election fraud for a variety of countries, states and counties. Ms. MacAlpine has served as an advisor for the office of the Secretary of State of California for the Risk Limiting Audit Pilot Program 2011-2012, and is widely regarded as an expert on the use of high-speed scanners for conducting post-election audits.

- **Kevin Collier, *Reporter, CNN***
  Kevin Collier is a reporter who covers the intersection of cybersecurity and national security, including efforts to safeguard election integrity. He has previously worked for BuzzFeed News, Vocativ, and the Daily Dot.

- **Kim Zetter, *Longtime cybersecurity/national security reporter for various publications including WIRED, Politico and The New York Times Magazine and author of the book* Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon**
  Kim Zetter is a longtime cybersecurity and national security reporter for various publications including Wired, Politico and the New York Times Magazine and author of the book Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. She has broken numerous national stories over the years about NSA surveillance, digital warfare, Wikileaks and the hacker underground, and has been one of the nation's leading journalists covering voting machine and election security since 2003.

- **Eric Geller, *Cybersecurity Reporter, Politico***
  Eric Geller is a journalist on Politico's cybersecurity team. His primary beat consists of cyber policymaking at the White House, the Justice Department, the State Department, and the Commerce Department, but he also regularly covers election security, data breaches, malware outbreaks, and other cyber issues affecting the government, the private sector, and society at large.

While the Bots Distracted You: Hacking the Electorate

Omelas and White Ops provide the most comprehensive ever look at the day to day tactics of Russian disinformation campaigns against elections. Using Omelas' subject matter expertise and AI, we show the extent of Russian propaganda shared on Reddit in the lead up to an election, the performance of different narratives and different domains, and the sentiment expressed in articles compared to the sentiment induced in the audience in comments. White Ops's state-of- the-art bot detection demonstrates how Russia has automated the process of spreading these narratives, the added reach attributable to bots, and the techniques employed by bots.

- **Evanna Hu, *CEO and Partner, Omelas***
  Evanna Hu is CEO and Partner of Omelas and non-resident Senior Fellow at the Atlantic Council. Omelas is a cutting edge technology company that exposes imminent risks among digital data. By utilizing machine learning/ artificial intelligence and data analytics, Omelas focuses on physical threats and identifies online campaigns of adversarial state and non-state actors. Evanna is also an expert in Counter-terrorism and Countering Violent Extremism, with fieldwork in Syria, Iraq, Afghanistan, Gaza, and Sweden, working on Neo-Nazi and Islamist violent extremists.

- **Ben Dubow, *CTO and President, Omelas***
  Ben Dubow is the CTO and President of Omelas. Ben began his career tracking the online propaganda of jihadists, Shiite extremists, white supremacists, and the militia movement before joining Google where he aided YouTube in detecting ISIS content, helped to develop Project SHIELD, and provided subject matter expertise for the Redirect Method. In 2017, Ben co-founded Omelas with the mission to stop the weaponization of the internet by providing precise data and analysis on how state actors and foreign terrorist organizations manipulate the web to achieve their geopolitical goals.

Trustworthy Elections: Evidence and Dispute Resolution

Suitably designed and operated paper-based voting systems can be strongly software independent, contestable, and defensible, and they can make risk-limiting audits and evidence-based elections possible. (These terms will be defined.) Not all paper-based voting systems have these properties. Systems that rely on ballot-marking devices and voter verifiable paper audit trails produced by electronic voting machines generally do not, because they cannot provide appropriate evidence for dispute resolution, which has received scant attention. An ideal system allows voters, auditors, and election officials to provide public evidence of any problems they observe--and can provide convincing public evidence that the reported electoral outcomes are correct despite any problems that might have occurred, if they are correct.

- **Philip Stark, *Professor of Statistics and Associate Dean of Mathematical and Physical Sciences, University of California, Berkeley***

  Philip B. Stark is Professor of Statistics and Associate Dean of Mathematical and Physical Sciences at the University of California, Berkeley. He works on inference and uncertainty quantification in many applications including the census, elections, information retrieval, and Internet filters. He also studies foundational questions in the philosophy of science and statistics. He developed "risk limiting audits" as a method to check election results, which are now in law in six states and required by pending federal legislation. Stark currently serves on the Board of Advisors of the U.S. Election Assistance Commission. He has testified as an expert witness in a range of civil and criminal cases on issues including antitrust, elections, employment, equal protection, food safety, intellectual property, product liability, and vaccines.

Keynote Remarks: Senator Ron Wyden (D-OR)

- **Senator Ron Wyden**

  Senator Ron Wyden is the foremost defender of Americans' civil liberties in the U.S. Senate, and a tireless advocate for smart tech policies. Years before Edward Snowden blew the whistle on the dragnet surveillance of Americans, Wyden warned that the Patriot Act was being used in ways that would leave Americans shocked and angry, and his questioning of NSA Director James Clapper in 2013 served as a turning point in the secret surveillance of Americans' communications.

  Since then, Wyden has fought to protect Americans' privacy and security against unwanted intrusion from the government, criminals and foreign hackers alike. He has opposed the government's efforts to undermine strong encryption, proposed legislation to hold companies accountable for protecting their users' data, and authored legislation with Rand Paul to protect Americans' Fourth Amendment rights at the border.

  Wyden is a senior member of the Senate Select Committee on Intelligence and the top Democrat on the Senate Finance Committee. He lives in Portland, Oregon.

If the Voting Machines are Insecure, Let's Just Vote on Our Phones!

Despite the consensus that Russian actors targeted multiple points of U.S. election infrastructure, there are persistent calls for voting over internet-connected devices. This is not new: 31 states and

the District of Columbia allow military and overseas voters to send voted materials to their home counties via the internet, including by fax and email. Now, several jurisdictions are piloting another internet system that allows voters to send their votes via a mobile application which stores those votes in a blockchain. Such programs undermine the efforts made since 2016 to secure the election administration offices from attacks. Our military and overseas voters need to successfully cast their ballots on time – but we owe it to them to find ways that do not increase the security risk.
This talk will take a look at the current landscape of election security leading into 2020, examining the implications that technologies like blockchain could have on our elections and what the role of responsible technology looks like on our voting infrastructure.

- **Marian Schneider, *President, Verified Voting***

  Marian Schneider is the president of Verified Voting, a role to which she brings a strong grounding in the legal and constitutional elements governing voting rights and elections, as well as experience in election administration at the state level. Immediately before becoming President of Verified Voting, Marian served as Special Advisor to Pennsylvania Governor Tom Wolf on Election Policy. Previously, Governor Wolf appointed her as the Deputy Secretary for Elections and Administration in the Pennsylvania Department of State where she served from February 2015 until May 2017.

  Throughout her legal career, Marian has focused on the intersection of civil rights and election law. Formerly, she was a Senior Attorney with Advancement Project's Voter Protection program and was trial counsel in Applewhite v. Commonwealth, successfully challenging Pennsylvania's restrictive photo ID law on behalf of voters as an unconstitutional infringement on the fundamental right to vote.

  Marian received her J.D. from The George Washington University, where she was a member of the Law Review, and earned her B.A. degree cum laude from the University of Pennsylvania.

State and Local Preparations on Election Security in the Aftermath of the Mueller Report

- **Eric Geller *(moderator), Cybersecurity Reporter, Politico***

  Eric Geller is a journalist on Politico's cybersecurity team. His primary beat consists of cyber policymaking at the White House, the Justice Department, the State Department, and the Commerce Department, but he also regularly covers election security, data breaches, malware outbreaks, and other cyber issues affecting the government, the private sector, and society at large.

- **Alex Padilla, *Secretary of State of California***

  Alex Padilla was sworn in as California's Secretary of State on January 5, 2015. He is committed to modernizing the office, increasing voter registration and participation, and strengthening voting rights.

  Padilla previously served in the California State Senate from 2006 to 2014 where he chaired the Committee on Energy, Utilities, and Communications. As chair, he shepherded legislation to combat climate change and create a greener and more sustainable economy. In 1999, at the age of 26, Padilla was elected to the Los Angeles City Council to represent the same east San

Fernando Valley community where he grew up. In 2001, his colleagues elected him to the first of three terms as Council President, becoming the youngest member and the first Latino to serve in this capacity.

- **Noah Praetz, *Election Consultant; former Director of Elections, Cook County, Illinois***

  Noah is an election consultant and the former Director of Elections for Cook County, Illinois. In this capacity he was responsible for the overall management of elections in one of the largest election jurisdictions in the country.

  Noah is an adjunct professor at DePaul University College of Law teaching Election Law and sits on the advisory board of the University of Chicago Harris Cyber Policy Initiative. Noah has presented extensively on Election Security, Sustainability, Election Day Management, Voter Registration Modernization and other Election Related items. He has also published articles on cyber security, election day administration and referendum law in Illinois.

- **Barb Byrum, Ingham County Clerk, Ingham County, Michigan**

  Barb Byrum is currently in her second term as Ingham County Clerk, serving as the county's chief elections official. As Clerk of one of the most populous counties in the State of Michigan, Byrum has successfully conducted 21 elections, 4 union elections, and the 2016 Presidential Recount. Byrum currently serves on Michigan's Election Security Commission, the Secretary of State's team of advisors tasked with strengthening and better securing elections in the state.

  Byrum has been a consistent advocate for the voting rights of qualified registered voters, with a focus on voting rights of military and overseas voters. Byrum serves on the Overseas Voting Initiative, which is a joint effort by the Federal Voting Assistance Program and Council of State Governments.

  Byrum graduated from Michigan State University with a Bachelor of Science degree in agribusiness management. She also holds a law degree from the MSU College of Law. Byrum previously served three terms as a Michigan State Representative. During her time in the Legislature, Byrum served as the ranking Democrat on the House Committee on Redistricting and Elections.

- **Amber McReynolds, Executive Director, National Vote at Home Institute**

  Amber McReynolds is the Executive Director for the National Vote At Home Institute and is the former Director of Elections for the City and County of Denver, Colorado. As one of the country's leading experts on election administration and policy, she has proven that designing pro-voter policies, voter-centric processes, and implementing technical innovations will improve the voting process for all voters. During her time in Denver, the Elections office was transformed into a national and international award-winning election office. Amber was also recognized as a 2018 Top Public Official of the Year by Governing Magazine for her transformational work to improve the voting experience in Denver and across Colorado. She is now focused on improving the voting experience across the country.

2020: Ready? Or Not?

- **Sherri Ramsay, *Senior Advisor, CyberPoint International; Senior Advisor: Cyber & NSA, Cambridge Global Advisors; former Director of the National Security Agency/Central Security Service Threat Operations Center (NTOC)***

  Sherri Ramsay is a consultant, engaged in cybersecurity strategy development and planning, cyber assessments, leadership, partnership development, and marketing & development of cybersecurity tools and security operations centers.

  Ms. Ramsay is the former Director of the National Security Agency's (NSA) Threat Operations Center. She led discovery and characterization of threats to national security systems, provided situational awareness for those threats, and coordinated actionable information to counter those threats with the Department of Defense, Department of Homeland Security, and Federal Bureau of Investigation. She also served as a senior leader in NSA's Signals Intelligence Directorate, Technology Directorate, and Information Assurance Directorate.

  Ms. Ramsay holds a Bachelor of Science degree from the University of Georgia, a Master of Science Degree from Johns Hopkins University, and Master's Degree from the Industrial College of the Armed Forces, National Defense University. She is on the Board of Advisors for Virginia Tech's Hume Research Center, the University of Chicago Cyber Policy Initiative, and TruSTAR Technology.

Beyond the Voting Machine: Other High Value Targets in Today's Election System

Since the U.S. Presidential election in 2016, there has been a heightened interest in election hacking. While electronic voting machines have been the primary focus, there are other high value targets could topple our election system if they were manipulated or compromised.

Brian will share his years of research into election systems to give you an insider's view of these high value targets and how and why they could be used by an adversary. In addition to a technical analysis of the components of an electronic voting machine, he will discuss the potential weaknesses of other key pieces of today's election system that many have overlooked.

- **Brian Varner, *Special Projects Researcher, Symantec Cyber Security Services***

  Since 2010 Brian Varner has been a special projects researcher on Symantec's Cyber Security Services team, leading the company's CyberWar Games and emerging technologies development. He previously worked at the National Security Agency as a tactical analyst.

  Brian holds a bachelor's degree in Computer Science from Florida Southern and master's degree in Information Assurance from Norwich University. Since early 2016, Brian has researched electronic voting machines and campaign security issues and is often called on by peers and media for his unique perspective on the potential threats facing today's election systems.

Putting Voters First: Expanding Options to Vote

- **Amber McReynolds, *Executive Director, National Vote at Home Institute***

  Amber McReynolds is the Executive Director for the National Vote At Home Institute and is the former Director of Elections for the City and County of Denver, Colorado. As one of the country's

leading experts on election administration and policy, she has proven that designing pro-voter policies, voter-centric processes, and implementing technical innovations will improve the voting process for all voters. During her time in Denver, the Elections office was transformed into a national and international award-winning election office. Amber was also recognized as a 2018 Top Public Official of the Year by Governing Magazine for her transformational work to improve the voting experience in Denver and across Colorado. She is now focused on improving the voting experience across the country.

Thirty Years Behind the Ballot Box: A firsthand look at the multiple factors preventing fair, effective and secure elections in America

- **Ion Sancho, *former Supervisor of Elections, Leon County, Florida***

  Ion Sancho served 28 years as Supervisor of Elections of Leon County, Florida. Elected in November of 1988, Sancho was sensitized to problems in elections when 5,000 voters were disenfranchised in a 1986 state and local primary election due to the misprogramming of the voting machines. Sancho was candidate in that election, and since then has dedicated his professional career to properly administering elections in Leon County, working for fair, accessible and verifiable elections nationwide.

  Concerned by voting machine security, Supervisor Sancho sanctioned a number of red team attacks on his voting system in the spring and summer of 2005, captured in HBO's 2007 Emmy-nominated documentary "Hacking Democracy", showing how the system could be hacked to alter the outcome of any election without being detected unless the paper ballots themselves were audited.

  Ion Sancho retired after the 2016 presidential election. He has remained active in the elections field, appearing as an expert witness in election cases and working with public and private entities heightening awareness to the threat of foreign intrusion to the American voting process, particularly the critical need for audits.

UnclearBallot: Automated Ballot Image Manipulation

As paper ballots and post-election audits gain increased adoption in the United States, election technology vendors are offering products that allow jurisdictions to review ballot images---digital scans produced by optical-scan voting machines---in their post-election audit procedures. Jurisdictions including the state of Maryland rely on such image audits as an alternative to inspecting the physical paper ballots.We show that image audits can be reliably defeated by an attacker who can run malicious code on the voting machines or election management system. Using computer vision techniques, we develop an algorithm that automatically and seamlessly manipulates ballot images, moving voters' marks so that they appear to be votes for the attacker's preferred candidate. Our implementation is compatible with many widely used ballot styles, and we show that it is effective using a large corpus of ballot images from a real election. We also show that the attack can be delivered in the form of a malicious Windows scanner driver, which we test with a scanner that has been certified for use in vote tabulation by the U.S. Election Assistance Commission. These results demonstrate that post-election audits must inspect physical ballots, not merely ballot images, if they are to strongly defend against computer-based attacks on widely used voting systems.

- **Kart Kandula, *Graduate Student, University of Michigan***
  Kart Kandula received his B.S.E. degree in computer science engineering from the University of Michigan in 2019 and is currently pursuing an M.S.E in the same area. He conducts research in the UM-Security lab under the supervision of Professor J. Alex Halderman. Currently, his research interest lies in problems affecting society and public policy, specifically election security. He has held internships at Microsoft and J.P. Morgan in the past.

- **Jeremy Wink, *Undergraduate Student, University of Michigan***
  Jeremy Wink is an undergraduate student at the University of Michigan currently pursuing a BSE in Computer Science. He has taken multiple security courses and has spent time researching topics surrounding election cybersecurity under J. Alex Halderman.

Saturday, August 10, 2019

Organizational Cybernetics: A Key to Resilience for the Digital Village

- **Kimberly Young-McLear, *Assistant Professor, U.S. Coast Guard Academy***
  Lieutenant Commander Kimberly Young-McLear is currently an Assistant Professor at the U.S. Coast Guard Academy. She holds engineering and technical degrees from Florida A & M, Purdue, and The George Washington University, including a Ph.D in Systems Engineering. She has taught a breadth of courses including Operations and Project Management, Crisis Mapping & Cybernetics, and Cybersecurity Risk Management. She has been instrumental in enhancing the inclusion of cybersecurity training and education program at the Academy for cadets and faculty. Lieutenant Commander Young-McLear was a key thought leader for the development of the Coast Guard Academy's first cyber undergraduate major. Furthermore as Vice Chair, she leads a multidisciplinary faculty Cyber Council to advance cyber curriculum and research at the Academy. Her research niche is focused on protecting critical infrastructure from cyber threats in the Maritime Domain. LCDR Young-McLear is also the program developer for NET21, a middle school outreach program, designed to systematically close STEM gaps amongst underrepresented students and teachers of color in the field of cybersecurity.

Ideas Whose Time Has Come: CVD, SBOM, and SOTA

From their origins in general purpose computing, Coordinated Vulnerability Disclosure (CVD), Software Bill of Materials (SBoM), and Secure Over-The-Air (SOTA) updates have been implemented or considered in safety sectors including industrial control systems, medical device manufacturing, and ground transportation. These common software security practices are becoming widespread global norms, turning up in public policy, international standards, and national law (often in sector-specific safety regulation). This talk will briefly review the practices (what), provide examples of successful implementations and supporting information (how), and (why).

- **Katie Trimble, *Section Chief, Vulnerability Management and Coordination, U.S. Cybersecurity and Infrastructure Security Agency, Department of Homeland Security***
  Katie Trimble currently serves as the Section Chief of the Vulnerability Management and

Coordination section of the Cyber Threat & Risk Analysis (CTRA) branch of the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC). In that capacity, she leads the Department's primary operations arm for coordination of the responsible disclosure and mitigation of identified cyber vulnerabilities in control systems and enterprise hardware and software used in the 16 critical infrastructure sectors and all levels of U.S. government organizations. Ms. Trimble started her career as an intelligence analyst with the United States Air Force, specializing in counterinsurgency, antiterrorism & force protection, counter explosive devices and communications systems. Ms. Trimble holds a Bachelors of Arts in International Relations & Global Studies from Antioch University Seattle.

- **Art Manion, *Vulnerability Analysis Technical Manager, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University***

  Art Manion is the Vulnerability Analysis Technical Manager at the CERT Coordination Center, part of the Software Engineering Institute at Carnegie Mellon University. He has studied software security and coordinated responsible disclosure efforts since joining CERT in 2001. Having gaining mild notoriety for saying "Don't use Internet Explorer" and "Replace CPU hardware" in public, Manion now focuses on policy, advocacy, and rational tinkering approaches to software security, including standards development in ISO, OASIS, and FIRST. Prior to joining CERT, Manion was the Director of Network Infrastructure at Juniata College.

Incident Lifecycle and Incident Response Management Planning

In the past few years, the volume, types, and quality of cybersecurity - related attacks in elections have become more damaging and disruptive, and new types of security-related incidents have emerged. This white paper describes the best-known method for analyzing the stages of cybersecurity incidents and identifies actions that can be taken to avoid or minimize impacts at each incident lifecycle stage. We discuss the overarching workflow for elections security incident response and management and describe the Point and Line analysis approach, which considers factors such as attack vectors, motives, probability, and imp act to develop a set of Incident Response Templates in this paper. In addition, we include reusable templates for analyzing cybersecurity Incident Lifecycle and Incident Response Management, which can be customized for specific needs of any election jurisdiction in this paper.

- **Rahul K. Patel, *Elections Information Security Officer, Office of the Cook County Clerk and Chicago Board of Elections Commissioners***

  Rahul Patel is a seasoned Cyber & Information Security professional with over 25 years of experience defending the availability, confidentiality, and integrity of information assets. He is presently leading elections information security and risk management efforts at the office of the Cook County Clerk and Chicago Board of Elections Commissioners as an Elections Information Security Officer. Patel holds a PhD from Northcentral University, an M.B.A. from DePaul University, and an M.S. from Illinois Institute of Technology

- **Tonya Rice, *Director of Elections, Cook County, Illinois***

  Tonya Rice was appointed Director of Elections by Cook County Clerk Karen A. Yarbrough in 2019,

in which capacity she supports operations for one of the largest election jurisdictions in the country. Rice began her career in elections in 2005 as a political science graduate student at the University of Michigan, where she was a National Science Foundation Graduate Research Fellow, specializing in public opinion on voting technology and post-election audits, as well as the political participation of language minority citizens. Rice holds a J.D. from Northwestern University School of Law and B.A. from Northwestern University.

Assessing Election Infrastructure

- **Jason Hill, *Chief, National Cybersecurity Assessments and Technical Services (NCATS)***
  Jason Hill is the Chief of the National Cybersecurity Assessment and Technical Services (NCATS) Branch of the Cybersecurity and Infrastructure Security Agency (CISA). In this capacity Jason has primary responsibility to deliver quality security testing and analysis to customers that include the Federal government, State, Local, Tribal and Territorial governments, as well as Private Sector/Critical Infrastructure stakeholders. Mr. Hill has worked with several tech companies creating and teaching red team course work and conducting penetration testing in the commercial industry and DOD. Jason also spent 22 years as a US Army National Guardsmen for the Commonwealth of Virginia. As Master Sergeant of the 91st Cyber Brigade he led the Cyber Opposition Forces which provides red team & pen testing capabilities. He has achieved certifications for the Offensive Security Certified Professional and the Certified Ethical Hacker trainings.

- **Genevieve Marquardt, *IT Specialist, National Cybersecurity Assessments and Technical Services (NCATS)***
  Genevieve Marquardt serves as a member of the National Cybersecurity Assessments and Technical Services (NCATS) Cyber Hygiene team which is responsible for continuously assessing the "health" of external stakeholders' endpoints reachable via the internet and maintaining an updated enterprise view of the cyber security posture of their systems to drive proactive mitigation of vulnerabilities and reduce risk. Genevieve provides technical support pertaining to public IP scans and testing of .gov public facing networks for stakeholders.

- **Derrick Thornton, *Federal Lead, National Cybersecurity Assessments and Technical Services (NCATS)***
  Derrick Thornton joined the National Cybersecurity Assessments and Technical Services (NCATS) team in June 2017 as an Information Security Specialist. Derrick serves as a Federal Lead leading NCATS RVA teams conducting two week penetration tests. An 11-year veteran of the U.S. Air Force, Derrick was stationed at Robins Air Force Base, Georgia and at White Sands Missile Range, New Mexico while also serving 2 tours in the Middle East. The 4 years of military service at White Sands Missile Range was an assignment to the National Reconnaissance Office, which led to a 21-year career within the NRO. Derrick has a Bachelor of Science in Technical Management from DeVry University.

Securing America: How DHS, States, and Cybersecurity Startups are Working Together Before the 2020 Presidential Election

In 2016, 50 states' election systems were targeted by Russian nation-state hackers. Russian actors visited election websites, tested vulnerabilities by trying to exploit SQL database vulnerabilities, and even managed to access voter registration files and a county ballot. DHS deemed US election infrastructure "critical" and now CISA, DHS' critical infrastructure office, is actively providing scanning technology and technical assistance to states. States, which have direct authority over the issue, are doing a great job with their own efforts including working with the National Guard, looking public-private partnerships to provide DDoS mitigation and in some cases trying bug bounties and working with ethical hackers to keep elections secure. However, there is still much to be done to secure our democratic/election systems before 2020 - we need YOU. Election security will require a united effort with the scale and vigilance of a crowd of top talent. How are states innovating before the 2020 Presidential Election? How can hackers help?

- **Joseph Marks *(moderator), Reporter, The Washington Post***
  Joe Marks is a reporter for The Washington Post, where he writes The Cybersecurity 202 newsletter focused on the policy and politics of cybersecurity. Before joining The Washington Post, Marks covered cybersecurity for Politico and Nextgov. He also covered patent and copyright trends for Bloomberg BNA and federal litigation for Law360. Marks began his career at Midwestern newspapers covering city and county governments, crime, fires and features. He spent two years at the Grand Forks Herald in North Dakota and is originally from Iowa City.

- **Rita Gass, *CIO, California Secretary of State's Office***
  Rita established her career and progressed throughout the roles to become a chief information officer in 2008 with CCC. Remaining in this role for eight years, she eventually moved to the same role with California Secretary of State (SOS), where she continues to work now.

- **Wayne Thorley, *Deputy Secretary for Elections, Nevada Secretary of State's Office***
  Wayne Thorley is the Deputy Secretary of State for Elections for the Nevada Secretary of State's office and is responsible for administering the Nevada's election process including enforcing state and federal election laws and procedures and the Help America Vote Act.

- **Trevor Timmons, *CIO, Colorado Secretary of State's Office***
  Trevor Timmons has served the Colorado Secretary of State as Chief Information Officer since 2007, after eight years as Deputy CIO and Director of Software Development. Mr. Timmons has served under several Secretaries of State, during which time Colorado has gained a national reputation in several areas, including elections administration and cybersecurity operations.

- **Alex Joves, *Regional Director, Region V, Cybersecurity and Infrastructure Security Agency***
  Alex Joves is the Regional Director for Region V of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. He has served in various roles for DHS since 2007, including Regional Supervisor of Chemical Facility Anti-Terrorism Standards and Director of the National Infrastructure Coordinating Center. Prior to joining DHS, Mr. Joves was an

Associate Attorney at Perkins Coie LLP. He has a JD from The George Washington University Law School and a Bachelor of Science in Government from the U.S. Coast Guard Academy.

- **Josh Benaloh, *Senior Cryptographer, Microsoft Research***
  Josh Benaloh is a Senior Cryptographer at Microsoft Research and has worked on verifiable election technologies for more than thirty years. His 1987 doctoral dissertation at Yale University, entitled "Verifiable Secret-Ballot Elections", introduced the use of homomorphic encryption as a means to enable public verifiability in elections.
  Dr. Benaloh served seventeen years on the Board of Directors of the International Association for Cryptologic Research and currently serves on the Coordinating Committee of the Election Verification Network. He has published and spoken extensively and testified before Congress on election technologies and was an author of the 2018 National Academies of Science, Engineering, and Medicine report "Securing the Vote – Protecting American Democracy".

- **Alissa Starzak, *Head of Policy, Cloudflare***
  Alissa Starzak is the Head of Public Policy at Cloudflare, an Internet performance and security company that is on a mission to help build a better Internet.

- **Jay Kaplan, *Co-Founder and CEO, Synack***
  Jay co-founded Synack after serving in several security-related capacities at the Department of Defense, including the DoD's Incident Response and Red Team.

Bootstrapping Vulnerability Disclosure for Election Systems

Seven months. It look seven months to make contact with a major city after discovering a critical vulnerability in their election registration website, which could have exposed (or worse, modified) information of millions of voters. As seen in the Mueller report, election systems are under active attack by foreign adversaries. Yet while vulnerability disclosure policies are becoming the norm in most industries, exactly zero states or election vendors have established vulnerability disclosure policies to allow reporting vulnerabilities in election systems. In a time where accepting feedback from the public is the best defense against these attacks, the lack of vulnerability disclosure policies hinders improvements in securing systems. In a talk by security researcher Jack Cable and Katie Trimble from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, learn industry best practices for vulnerability disclosure and how election systems can benefit from additional public scrutiny. Hear Jack's experiences disclosing critical vulnerabilities in several major election registration systems, and how this can be channeled to protect our nation ahead of the 2020 elections.

- **Jack Cable, *Security Researcher and Student, Stanford University***
  Jack Cable is a coder turned white hat hacker and a rising sophomore at Stanford University. Jack is a top ranked hacker on the HackerOne bug bounty platform, having identified over 350 vulnerabilities in companies including Google, Facebook, Uber, Yahoo, and the U.S. Department of Defense. After placing first in the Hack the Air Force challenge, Jack began working this past summer at the Pentagon's Defense Digital Service. At Stanford, Jack studies computer science and launched Stanford's bug bounty program, one of the first in higher education.

- **Katie Trimble, *Section Chief, Vulnerability Management and Coordination, U.S. Cybersecurity and Infrastructure Security Agency, Department of Homeland Security***
  Katie Trimble currently serves as the Section Chief of the Vulnerability Management and Coordination section of the Cyber Threat & Risk Analysis (CTRA) branch of the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC). In that capacity, she leads the Department's primary operations arm for coordination of the responsible disclosure and mitigation of identified cyber vulnerabilities in control systems and enterprise hardware and software used in the 16 critical infrastructure sectors and all levels of U.S. government organizations. Ms. Trimble started her career as an intelligence analyst with the United States Air Force, specializing in counterinsurgency, antiterrorism & force protection, counter explosive devices and communications systems. Ms. Trimble holds a Bachelors of Arts in International Relations & Global Studies from Antioch University Seattle.

- **Trevor Timmons, *CIO, Colorado Secretary of State's Office***
  Trevor Timmons has served the Colorado Secretary of State as Chief Information Officer since 2007, after eight years as Deputy CIO and Director of Software Development. Mr. Timmons has served under several Secretaries of State, during which time Colorado has gained a national reputation in several areas, including elections administration and cybersecurity operations.

"The Election System: Can We Fix It?" "YES WE CAN!"

As the previous DEF CON Voting Villages have proved, our voting equipment and infrastructure are very vulnerable to multiple types of attacks. Instead of focusing on problems and broken things, this talk will focus on simple fixes that vendors and governments can put into action right now.
Starting with the machines themselves, then moving through parts of the entire system, BiaSciLab will offer suggestions on how simple practices and changes in thinking and hiring can improve the security of the entire system.
Last year at r00tz BiaSciLab was one of the first to hack the mock election reporting system set up by the Voting Village. Some have pointed out that this was a purposely flawed system designed for the the kids to break. However, as outlined in the Mueller report, Russian hackers used the same SQL injection technique to break into an election reporting system. If our systems are so secure, how was this able to happen? Lack of secure coding practices and both peer and outside review. If proper coding review and application testing had happened, this SQL injection vulnerability would have been found and fixed.
Breaking down these flaws and offering real solutions for each one, BiaSciLab will bring hope in the face of this daunting and complex security problem.

- **BiaSciLab, *Founder and CEO, Girls Who Hack***
  BiaSciLab is a 12 year old hacker and maker. She was the youngest speaker at the Hackers on Planet Earth conference and has spoken at DEF CON previously in both the Bio Hacking Village and the r00tz Asylum kids con. She received national attention when she hacked the voting reporting system at DEF CON 26. BiaSciLab is alsothe Founder and CEO of Girls Who Hack, an organization focused on teaching girls the skills of hacking so that they can change the future.

Securing Voting Systems (Beyond Paper Ballots!)

While much "headline hacking" is devoted to exposing vulnerabilities on voting machines themselves, there is more to election systems security than simply popping shells on old, unsupported kiosks. In this session, attendees will learn what real world IT personnel in the 3071 counties and parishes across the U.S. face on and around Election Day, beyond the voting machine.

- **Tod Beardsley, *Director of Research, Rapid7***

  Tod Beardsley is the Director of Research at Rapid7. He has over 30 years of hands-on security experience, stretching from in-band telephony switching to modern Internet of Things implementations. He has held IT Operations and Security positions in large organizations such as 3Com, Dell, and Westinghouse, as both an offensive and defensive practitioner.

Machine Voting: The Bulgarian Experience

First machine voting experiments in Bulgaria started in 2009. Since then machine voting found its place in legislation with the usage of offline DRE kiosks with VVPAT. Latest developments in information security and the rising threads require flexible technical approach with still lagging legislation. The talk will pass through our machine voting experience, problems and solutions we came up with. We'll share detailed security requirements for voting machines and their implementation in practice. Special emphasis will be put on latest European parliament elections, held in May 2019 and upcoming municipal elections in October 2019.

- **Alex Stanev, *CTO, Information Services JSC***

  Alex started as a software developer in late 90s working on a wide range of projects – from specialized hardware drivers to large scale information systems for private and public sectors, including e-government services, elections management and smart cities.

  Since 2003 Alex has been leading computer processing of all election results and referendum projects in Bulgaria. As a consultant for the Central Election Commission of Bulgaria Alex is the primary author of technical and security requirements for election machines used in Bulgaria. As a security consultant, Alex has lead penetration test audits in Europe, America and Africa for financial and government institutions.

  Currently Alex serves as CTO in the largest Bulgarian systems integrator - Information Services JSC.

Addressing the election security threats posed by Very Small Jurisdictions

While most election administrators in the US are working in jurisdictions with populations in the tens or hundreds of thousands, there are states with jurisdictions as small as a dozen or so voters. In these Very Small Jurisdictions, the local interface with the state election system can be as crude as a Windows XP computer directly connected to an ISP and used by an Election Administrator with little computer experience or understanding of anti-social engineering practices. These are administrators with direct user access to statewide election systems containing voter roles and responsible for posting official election results. And while there are creative approaches to improving election worker training to offset social engineering threats underway in several states, they are virtually all designed for the more typical "macro" jurisdiction level (country-level

jurisdictions) and are not scaleable to these "micro" levels, leaving secretaries of state to run generalized safety trainings with little follow-up and few options for addressing these vulnerabilities. The talk will briefly explore the threat and why creating public logical network structures are best suited not just to mitigate the problem, but to potentially make these jurisdictions even more secure than their larger counterparts.

- **John Odum, *CMC, CEH, CNDA, MCP, CIW; City Clerk, Montpelier, Vermont***
  John Odum has been the elected City Clerk of Vermont's Capital, Montpelier, for 7 years. In this capacity he also serves as the the Election Administrator for Montpelier. Prior to being elected clerk, John worked in communications and IT for non-profits and political campaigns. His work has been published on websites of The Guardian, Governing, Huffington Post, as well as numerous Vermont area publications.

The Devil Went Down to Georgia. Did He Steal Souls? (Georgia's Electronic Voting Saga)

- **Marilyn Marks, *Executive Director, Coalition for Good Governance***
  In 2009, after a narrow loss to become the Mayor of Aspen, Marilyn Marks recognized the vulnerabilities in Colorado's election systems and chose to devote herself full time to election integrity litigation and lobbying efforts for more transparent and verifiable elections. She successfully litigated the effort to make Colorado ballots open public records for postelection reviews, followed by more than 25 election-related cases involving election transparency or voter privacy. She is currently the driving force behind the legal challenge to Georgia's unverifiable electronic voting system.

- **Rich DeMillo, *Professor of Computer Science and Executive Director, Center for 21st Century Universities, Georgia Tech***
  Richard DeMillo is the Charlotte B. and Roger C. Warren Chair of Computer Science and Professor of Management at Georgia Tech, where he founded and now directs the Center for 21st Century Universities. The Center is Georgia Tech's living laboratory for fundamental change in higher education. He is responsible for educational innovation at Georgia Tech and is a national leader and spokesman in the online revolution in higher education. Under his leadership, Georgia Tech has developed a pipeline of 50 Massive Open Online Courses that together enroll a million learners.

- **Logan Lamb, *Cybersecurity researcher***
  Logan Lamb is a Senior Security Engineer at Bird. Previously he has served as a Cyber Security Researcher at Bastille Networks and Oak Ridge National Laboratory. He has Master of Science and Bachelor of Science degrees in Computer Engineering, both from the University of Tennessee, Knoxville.

- **Jordan Wilkie, *Freelance journalist covering election integrity***
  Jordan Wilkie is pursuing a career as an investigative journalist covering criminal and social justice by combining data-driven reporting with long-form, narrative storytelling. My expertise to-date is in incarcerated juvenile and LGBTQ populations.

- **Robert McGuire, *Attorney for Coalition plaintiffs***

  Robert McGuire is the attorney for the National Election Defense Coalition plaintiffs in their current legal challenge to Georgia's unverifiable electronic voting system. His previous experience includes serving as a Senior Associate at Allen & Overy LLP, as a lecturer at the University of Denver's Sturm College of Law, and as a law clerk for the U.S. Court of Appeals for the Eighth Circuit. He earned his JD from Yale Law School.

- **Susan Greenhalgh *(moderator), Vice President of Policy and Programs, National Election Defense Coalition***

  Susan Greenhalgh is Vice President for Programs at National Election Defense Coalition. Susan performs extensive research, assembling and reviewing documents that may influence and impact state and federal policy regarding election verifiability and security. She also works with cyber security experts and advisors on the federal level to bridge the gap between national cyber security policy and election administration. Susan has a bachelor's degree from the University of Vermont in chemistry.

Sunday, August 11, 2019

Exploring Voter Roll Manipulation and Fraud Detection with Voter Files

Qualified Voter Files are published by states and contain information on registered voters. These files are used by political campaigns and analysts to gather data on registered voters. The public nature of these files also makes it easier for the public to detect voter fraud and can be used by third parties to help detect large scale voter registration attacks. The data contained in these files, however, could be used by attackers to impersonate voters and update or delete a voter's registration information and subsequently prevent the targeted voters from exercising their right to vote. Use of Qualified Voter Files could also inform attackers on what scale voters' information could be changed without raising suspicion.

- **Nakul Bajaj, *High School Researcher, University of Michigan***

  Nakul Bajaj is a rising high school senior at The Harker School. He is interested in computer science and public policy, and frequently participates in hackathons and debate competitions to learning more about each of these fields. Previously, he has done analysis on election datasets, finding patterns between race and income and voter turnout. In addition, he has worked on projects dealing with a combination of law and computer science, having built an expert system that helps inventors file their own patents. This summer, he is helping conduct research in Professor J. Alex Halderman's lab at the University of Michigan regarding electronic voting machines and other election security topics with help from PhD candidate Matthew Bernhard.

Defending Democracy: Working with Election Officials to Improve Election Security

Four years after documented foreign interference in the 2016 presidential election put election security in the headlines, cybersecurity experts and election officials still face challenges in working together. The need for collaboration is clear - especially in smaller and less well-resourced jurisdictions - so how can we bridge the gap? Hear from current and former election officials and election security advocates about how successful partnerships have moved the needle, and what to do if you want to engage your local election office.

- **Liz Howard, Counsel, *Democracy Program, Brennan Center for Justice***
  Liz Howard currently serves as Counsel for the Brennan Center's Democracy Program, with a focus on cybersecurity and elections. Prior to joining the Brennan Center, Ms. Howard was Deputy Commissioner for the Virginia Department of Elections. During her tenure overseeing election modernization projects in Virginia, she coordinated the state's decertification of all paperless voting systems, implementation of the e-Motor Voter program, and adoption of online, paperless absentee ballot applications. Ms. Howard earned her J.D. from the William & Mary School of Law in 2009.

- **Justin Burns, *Chief Information Security Officer, Washington Secretary of State***
  Justin Burns joined the elections security community in January, as CISO for the Washington Secretary of State. Prior to this, he served as a Solutions Architect and Technical Assistant to the Washington State CIO.

- **Trevor Timmons, *Chief Information Officer, Colorado Secretary of State***
  Trevor Timmons became Chief Information Officer for the Colorado Secretary of State in 2007, after eight years as Deputy CIO and Director of Software Development. During this time, Mr. Timmons served under several Secretaries of State and Colorado gained a national reputation in several areas, including elections administration and cybersecurity operations.

- **Jared Dearing, *Executive Director, Kentucky State Board of Elections***
  Jared Dearing is the Executive Director of the Kentucky State Board of Elections and has worked in the elections space for over ten years. Jared has public and private sector experience working both at the local and state level, including working for the City of Louisville as well as the Office of California Governor Jerry Brown. His private sector work includes several tech startups located in the Bay Area and Boston. He is a graduate of the University of California, Berkeley where he studied public policy and engineering.

- **Monica Childers *(moderator), Product Manager for Risk-Limiting Audits, VotingWorks***
  Monica Childers is a civic technologist with a background in digital product design and project management. As Product Manager at the VotingWorks she champions collaborative design, partnering with state and local election officials to build low cost, flexible tools for election administration. Over the past decade she has designed online voter engagement platforms, vote-by-mail ballot tracking systems, text & email election reminders, and a national trouble-ticket system for reporting problems with election mail. Having served as the project manager for Colorado's post-election audit software for the past year, she is currently working with election officials implementing risk-limiting audits (RLAs) and is helping shepherd the development of nationwide RLA software.

Securing Your Election Infrastructure: Plan and Prepare to Defend Your Election Systems, People, and Processes

Robert Anderson will provide some background of Election Security and the threat research that is on-going for Election Security. An overview for election teams to plan and prepare to defend their

Election Systems, People, and Processes. Provide guidance to update your Security Policies and Incident Response Plan. Help election teams understand their Attack Surface and where your election systems are most vulnerable. Review the primary Threat Actors poised to attack your election systems. Then review several approaches that could be deployed to protect Election Security Assets, and direct to some organizations that could support election teams.

- **Robert Anderson, *Chief Cyber Security Practitioner and President, Preying Mantis***
  Robert Anderson is a highly trained IT & Cyber Security professional with over 25 years of experience in a variety of cybersecurity domains. As a former Intelligence Officer working in the Middle East, he brings a unique perspective to security operations and incident response. Robert has deployed and led over 500 security programs and projects to Fortune 500 companies, federal, state, and local governments, and NATO. Robert has over 15 years hacking experience and is a Certified Ethical Hacker. He is an expert in Cyber Threat Intelligence and Information Warfare and has led Incident Response Teams during many high-profile breaches.

Keynote Remarks: Representative Eric Swalwell (CA-15)

- **Representative Eric Swalwell (CA-15)**
  In 2012 Eric Swalwell was elected to represent California's Fifteenth Congressional District, which includes a large part of the East Bay. Now in his fourth term, he's working hard to bring new energy, ideas, and a problem-solving spirit to Congress, with a focus on advancing policies that support equality, opportunity, and security.
  Congressman Swalwell serves on the House Permanent Select Committee on Intelligence, and believes protecting Americans is Congress' most solemn duty. He chairs the Intelligence Modernization and Readiness Subcommittee, which oversees overall management of the Intelligence Community: the policies and programs focused on making sure that all 17 U.S. intelligence agencies have the workforce, infrastructure and services they need to succeed. This involves fostering greater collaboration and better use of resources across the entire Intelligence Community in personnel management, security clearance reform, information technology modernization, and other areas.

Exhibit
PX 0057
Rion

OAN
YOUR NATION. YOUR NEWS

'DOMINION-IZING' THE VOTE

ONE AMERICA NEWS INVESTIGATES

Scientists say no credible evidence of computer fraud in the 2020 election outcome, but policymakers must work with experts to improve confidence

16 November 2020

We are specialists in election security, having studied the security of voting machines, voting systems, and technology used for government elections for decades.

We and other scientists have warned for many years that there are security weaknesses in voting systems and have advocated that election systems be better secured against malicious attack. As the National Academies recently concluded, “There is no realistic mechanism to fully secure vote casting and tabulation computer systems from cyber threats.” However, notwithstanding these serious concerns, we have never claimed that technical vulnerabilities have actually been exploited to alter the outcome of any US election.

Anyone asserting that a US election was “rigged” is making an *extraordinary* claim, one that must be supported by persuasive and verifiable evidence. Merely citing the existence of technical flaws does not establish that an attack occurred, much less that it altered an election outcome. It is simply speculation.

The presence of security weaknesses in election infrastructure does not by itself tell us that any election has actually been compromised. Technical, physical, and procedural safeguards complicate the task of maliciously exploiting election systems, as does monitoring of likely adversaries by law enforcement and the intelligence community. Altering an election outcome involves more than simply the existence of a technical vulnerability.

We are aware of alarming assertions being made that the 2020 election was “rigged” by exploiting technical vulnerabilities. However, in every case of which we are aware, these claims either have been unsubstantiated or are technically incoherent. To our collective knowledge, no credible evidence has been put forth that supports a conclusion that the 2020 election outcome in any state has been altered through technical compromise.

That said, it is imperative that the US continue working to bolster the security of elections against sophisticated adversaries. At a minimum, all states should employ election security practices and mechanisms recommended by experts to increase assurance in election outcomes, such as post-election risk-limiting audits.

If you are looking for a good place to start learning the facts about election security, we recommend the recent National Academies of Science, Engineering, and Medicine (NASEM) study, “Securing the Vote”, which is available for free download at https://doi.org/10.17226/25120.

Signed,

(Affiliations are for identification purposes only; listed alphabetically by surname.)

1. Tony Adams, Independent Security Researcher
2. Andrew W. Appel, Professor of Computer Science, Princeton University
3. Arlene Ash, Professor, University of Massachusetts Medical School
4. Steven M. Bellovin, Percy K. and Vida L.W. Hudson Professor of Computer Science; affiliate faculty, Columbia Law, Columbia University
5. Matt Blaze, McDevitt Chair of Computer Science and Law, Georgetown University
6. Duncan Buell, NCR Professor of Computer Science and Engineering, University of South Carolina
7. Michael D. Byrne, Professor of Psychological Sciences and Computer Science, Rice University
8. Jack Cable, Independent Security Researcher
9. Jeremy Clark, NSERC/Raymond Chabot Grant Thornton/Catallaxy Industrial Research Chair in Blockchain Technologies, Concordia Institute for Information Systems Engineering
10. Sandy Clark, Independent Security Researcher
11. Stephen Checkoway, Assistant Professor of Computer Science, Oberlin College
12. Richard DeMillo, Chair, School of Cybersecurity and Privacy and Warren Professor of Computing, Georgia Tech
13. David L. Dill, Donald E. Knuth Professor, Emeritus, in the School of Engineering, Stanford University
14. Zakir Durumeric, Assistant Professor of Computer Science, Stanford University
15. Aleksander Essex, Associate Professor of Software Engineering, Western University, Canada
16. David Evans, Professor of Computer Science, University of Virginia
17. Ariel J. Feldman, Software Engineer
18. Edward W. Felten, Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University
19. Bryan Ford, Professor of Computer and Communication Sciences, Swiss Federal Institute of Technology Lausanne (EPFL)
20. Joshua M. Franklin, Independent Security Researcher
21. Juan E. Gilbert, Banks Family Preeminence Endowed Professor & Chair, University of Florida
22. J. Alex Halderman, Professor of Computer Science and Engineering, University of Michigan
23. Joseph Lorenzo Hall, SVP Strong Internet, Internet Society
24. Harri Hursti, co-founder Nordic Innovation Labs and Election Integrity Foundation
25. Neil Jenkins, Chief Analytic Officer, Cyber Threat Alliance
26. David Jefferson, Lawrence Livermore National Laboratory (retired)
27. Douglas W. Jones, Associate Professor of Computer Science, University of Iowa

28. Joseph Kiniry, Principal Scientist, Galois, CEO and Chief Scientist, Free & Fair
29. Philip Kortum, Associate Professor of Psychological Sciences, Rice University
30. Carl E. Landwehr, Visiting Professor, University of Michigan
31. Maggie MacAlpine, co-founder Nordic Innovation Labs and Election Integrity Foundation
32. Bruce McConnell, former Deputy Under Secretary for Cybersecurity, Department of Homeland Security, (currently) President, EastWest Institute
33. Patrick McDaniel, Weiss Professor of Information and Communications Technology, Penn State University
34. Walter Mebane, Professor of Political Science and of Statistics, University of Michigan
35. Eric Mill, Chrome Security PM, Google
36. David Mussington, Professor of the Practice, School of Public Policy, University of Maryland College Park
37. Peter G. Neumann, Chief Scientist, SRI International Computer Science Lab
38. Lyell Read, Researcher at SSH Lab, Oregon State University
39. Ronald L. Rivest, Institute Professor, Massachusetts Institute of Technology
40. Aviel D. Rubin, Professor of Computer Science, Johns Hopkins University
41. Bruce Schneier, Fellow and Lecturer, Harvard Kennedy School
42. Alexander A. Schwarzmann, Dean of Computer and Cyber Sciences, Augusta University
43. Hovav Shacham, Professor of Computer Science, The University of Texas at Austin
44. Micah Sherr, Provost's Distinguished Associate Professor, Georgetown University
45. Barbara Simons, IBM Research (retired)
46. Kevin Skoglund, Chief Technologist, Citizens for Better Elections
47. Michael A. Specter, EECS PhD Candidate, MIT
48. Alex Stamos, Director, Stanford Internet Observatory
49. Philip B. Stark, Professor of Statistics and Associate Dean of Mathematical and Physical Sciences, University of California, Berkeley
50. Jacob Stauffer, Director of Operations, Coherent CYBER
51. Camille Stewart, Cyber Fellow, Harvard Belfer Center
52. Rachel Tobac, Hacker, CEO of SocialProof Security
53. Giovanni Vigna, Professor, Computer Science, University of California, Santa Barbara
54. Poorvi L. Vora, Professor of Computer Science, The George Washington University
55. Dan S. Wallach, Professor, Departments of Computer Science and Electrical & Computer Engineering, Rice Scholar, Baker Institute of Public Policy, Rice University
56. Tarah Wheeler, Cyber Fellow, Harvard Belfer Center
57. Eric Wustrow, Assistant Professor, Department of Electrical, Computer & Energy Engineering, University of Colorado Boulder
58. Ka-Ping Yee, Review Team Member, California Secretary of State's Top-to-Bottom Review of Voting Systems
59. Daniel M. Zimmerman, Principal Researcher, Galois and Principled Computer Scientist, Free & Fair


Exhibit
PX 0059
Rion
OAN
YOUR NATION, YOUR NEWS
RON WATKINS
LARGE SYSTEMS TECHNICAL ANALYST
ONE AMERICA NEWS
INVESTIGATES

Tweets 2,163 | Following 346 | Followers 172K | Likes 981

Follow

Ron

@CodeMonkeyZ

free speech absolutist | susucoin | former 8kun admin (resigned november 3, 2020)

Joined September 2013

Tweets | Tweets & replies | Media

Pinned Tweet

Ron @CodeMonkeyZ · Nov 3

I am resigning as admin of 8kun effective immediately.
Extensive battles have been fought tooth and nail during a self-imposed civic duty protecting the final fortifications of online free speech, guardedly navigating these tumultuous times.
Today I bring ship to dock.

Farewell.

Ron @CodeMonkeyZ · 46m

If you were an election official in Pennsylvania who was trained to work on the Dominion Voting System, please contact me. Im interested in learning about what training you had regarding the technical aspects of the Dominion system.

Ron @CodeMonkeyZ · 2h

Ms. Chanel Rion just reached out to me and Ill be talking with her about Dominion tomorrow.

Ron @CodeMonkeyZ · 2h

Ballots are 100% interlinked with the voting software. Sending a blank ballot allows the software to tabulate votes differently from a ballot that is correctly populated.

Whether these blank ballots were used for fraud is an exercise for investigators to prove.

Philly GOP @PhillyGOP
Voters in Allentown, PA are receiving blank ballots!! WIDESPREAD!

🚨🚨Have you received a blank ballot? Email us photos

Ron @CodeMonkeyZ · 3h

If I had forensic access to the live configuration data, logs, settings, and intranet setup of the Dominion voting system used in the districts reporting anomalies, im confident I could quickly and conclusively blow the lid off digital election fraud if it had actually occurred.

Ron @CodeMonkeyZ · 3h

Ive reached out to @RudyGiuliani offering to give him a 15 minute phone briefing on where I think he might be able to uncover end-user fraud within the Dominion voting system.
I can give him a simple road map of what he might want to look at with a bit more scrutiny.

Ron @CodeMonkeyZ · 4h

Just for the record, I am not alleging voter fraud. I have no proof of voter fraud. All I am doing is reading the election machine manuals and security audits and making independent observations about how the systems could potentially be used for fraud.

Ron @CodeMonkeyZ · 4h

Where are our checks and balances for the local IT guy? Who is auditing his actions? Where are the logs? Which settings did he enable? Did he change settings? When?

Show this thread

Ron @CodeMonkeyZ · 4h

The software seems to be legit and written well. It passes independent security audits and probably works as intended.
The issue is the amount of control the software gives to the local IT guy who can ultimately decide the fate of a nation.

Show this thread

Ron @CodeMonkeyZ · 4h

The absurd amount of "settings" on the Dominion Voting Software is off-the-charts.

If I was a local IT guy, I could probably setup the voting machine to give myself an elected position without ever being on any ballot or running any campaign.

Show this thread

Ron @CodeMonkeyZ · 4h

More to come later.
Many people have sent me (completely publicly available) Dominion security audits, documents, manuals, and state contracts. Have a lot of reading to do.

If there are any potential election fraud settings hiding in plain sight, I will do my best to find it.

Show this thread

Ron @CodeMonkeyZ · 4h

9. There is an option to force the vote scanner to "overrun" a preset amount of ballots EVERY time anybody pauses the scan mid-batch. "Overrun" is undefined. Potential for abuse is high with this function, which was added shortly after 2018 mid-term elections.

Show this thread

Ron @CodeMonkeyZ · 4h

8. State of Pennsylvania requested semantic changes to the Dominion voting software, possibly to aid in their lawfare efforts. The word "Cast" became "Print", obfuscating the moment when your vote becomes officially cast. For what reason is currently unknown.

Show this thread

Ron @CodeMonkeyZ · 4h

7. Settings could theoretically have been changed during evening downtime on first night of voting. Much easier to change settings on hundreds of machines than to forge thousands of ballots. A couple of people could have done it quickly.

Show this thread

Ron @CodeMonkeyZ · 4h

6. Dominion is a black box with votes ultimately tabulated in a central server system. Who has access to the central server and where is the manual and security reviews of that server software?

Show this thread

Ron @CodeMonkeyZ · 4h

5. Local IT guys have ultimate power to clandestinely change settings, thus having the ability to potentially alter an entire election. There are no checks and balances or observers of the local IT guy when he accesses machine debug and admin settings. Its unclear if logs exist.

Show this thread

Ron @CodeMonkeyZ · 4h

4. Cryptic "split rotation" function that features the ability to "force a maximum deviation". There is no definition of a "split rotation", so we cannot know what "force a maximum deviation" means in this instance.

Show this thread

Ron @CodeMonkeyZ · 4h

3. Digital certificates are not protected by password, and Dominion user manual explicitly says not to enter a password. This enables potential for bad actors to MITM attack data traveling over network between precinct tabulator and central tabulator.

Show this thread

Ron @CodeMonkeyZ · 4h

2. Network Security is very weak since all software access keys use the same cryptographic pair. This gives plausible deniability to whoever potentially decides to mess around with voting settings. It cant be proven who changed a setting since everybody has the same key

Show this thread

Ron @CodeMonkeyZ · 4h

1. Votes can theoretically be ignored for individuals if a straight ticket vote is selected. This setting could very well enable "Republican"-style typo fraud. Many complex rules decide how the "straight ticket" option works.

Show this thread

Ron @CodeMonkeyZ · 4h

What we have learned so far from reading the Dominion Voting System manual:

Show this thread

New to Twitter?

Sign up now to get your own personalized timeline!

Sign up

Exhibit
PX 0060
Rion

Updated: November 17, 2020

SETTING THE RECORD STRAIGHT: FACTS & RUMORS

DOMINION VOTING SYSTEMS CATEGORICALLY DENIES FALSE ASSERTIONS ABOUT VOTE SWITCHING AND SOFTWARE ISSUES WITH OUR VOTING SYSTEMS.

According to a Joint Statement by the federal government agency that oversees U.S. election security, the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA): "There is no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised." The government & private sector councils that support this mission called the 2020 election "the most secure in American history."

1) VOTE DELETION/SWITCHING ASSERTIONS ARE COMPLETELY FALSE.

An unsubstantiated claim about the deletion of 2.7 million pro-Trump votes that was posted on the Internet and spread on social media has been taken down and debunked by independent fact-checkers.

- Edison Research (ER) has refuted any claims that company data suggests any voting irregularities, including vote switching. Edison Research President Larry Rosin told The Dispatch Fact

Check, *"Edison Research created no such report and we are not aware of any voter fraud."*

- Claims that 941,000 votes for President Trump in Pennsylvania were deleted are impossible. The fourteen counties using Dominion systems collectively produced 1.3 million votes, representing a voter turnout of 76%. Fifty-two percent of those votes went to President Trump, amounting to 676,000 votes processed for the President in Pennsylvania using company systems.
- Dominion ***does not*** have the ability review votes in real time as they are submitted.
- The U.S. Department of Homeland Security's cybersecurity division has confirmed that it is not possible for a bad actor to change election results without detection.

2) ASSERTIONS OF "SUPERCOMPUTER" ELECTION FRAUD CONSPIRACIES ARE 100% FALSE.

The Cybersecurity and Infrastructure Security Agency (CISA) has debunked claims about the existence of a secret CIA program for vote fraud called Hammer and Scorecard.

- All U.S. voting systems must provide assurance that they work accurately and reliably as intended under federal U.S. EAC and date certifications and testing requirements. Election safeguards - from testing and certification of voting systems, to canvassing and auditing - prevent malicious actors from tampering with vote counts and ensure final vote tallies are accurate. Read more from CISA.
- There have been no "raids" of Dominion servers by the U.S. military or otherwise, and Dominion does not have servers in Germany. CISA has refuted this claim on Twitter, and the U.S. Army has also confirmed to the Associated Press that it's false.

3) THERE WERE NO DOMINION SOFTWARE GLITCHES AND BALLOTS

WERE ACCURATELY TABULATED. THE RESULTS ARE 100% AUDITABLE.

No credible reports or evidence of any software issues exist. Dominion equipment is used by county and state officials to tabulate ballots. Human errors related to reporting tabulated results have arisen in a few counties, including some using Dominion equipment, but appropriate procedural actions have been taken by the county to address these errors were made prior to the canvass process.

- The Michigan Secretary of State's office offers a Fact Check Page which debunks false or erroneous claims about voting in Detroit, as well as a user-error incident in Antrim County.
- The Georgia Secretary of State has also repeatedly stated throughout the count that *"[a]s the work goes on, I want to assure Georgia voters that every legal vote was cast and accurately counted."*
- Dominion's systems are not responsible for 2,631 uncounted ballots discovered in Floyd County, Georgia during the statewide recount. The Secretary of State's office has cited clerical error and lack of following proper procedures as the cause.

4) DOMINION IS A NONPARTISAN U.S. COMPANY.

Dominion has no company ownership relationships with the Pelosi family, Feinstein family, Clinton Global Initiative, Smartmatic, Scytl, or any ties to Venezuela. Dominion works with all U.S. political parties; our customer base and our government outreach practices reflect this nonpartisan approach.

- As reported by the Associated Press, *"Dominion made a one-time philanthropic commitment at a Clinton Global Initiative meeting in 2014, but the Clinton Foundation has no stake or involvement in Dominion's operations, the nonprofit confirmed."* The meeting included bipartisan attendees focused on international democracy-building.

5) DOMINION IS NOT, AND HAS NEVER BEEN, OWNED BY SMARTMATIC.

Dominion is an entirely *separate company* and a *fierce competitor* to Smartmatic.

- Dominion and Smartmatic do not collaborate in any way and have no affiliate relationships or financial ties.
- Dominion does not use Smartmatic software.
- The only associations the companies have ever had were:
  - In 2009, Smartmatic licensed Dominion machines for use in the Philippines. The contract ended in a lawsuit.
  - In 2010, Dominion purchased certain assets from Sequoia, a private U.S. Company. Smartmatic, a previous owner of Sequoia, pursued legal actions against Dominion.

6) NO UNAUTHORIZED OR LAST-MINUTE SOFTWARE UPDATES OCCURRED.

Claims about software updates being done the night before Election Day are 100% false.

- Both Spalding County and the Georgia Secretary of State have verified that a) this type of unauthorized update is impossible, and b) the actual logs from equipment under the custody of the County determined an update did NOT happen the night before the election.
- Georgia Voting System Implementation Manager Gabe Sterling has affirmed in his daily press briefing on November 9 that *"nothing was done to the [PollPad] system after [October 31],"* when voter files were updated as part of normal procedure.

7) THERE ARE NO ISSUES WITH THE USE OF SHARPIE PENS.

Election officials provide writing instruments that are approved for marking ballots to all in-person voters using hand-marked paper ballots. Dominion Voting Systems

machines can read all of these instruments, including Sharpies.

- The DHS Cybersecurity and Infrastructure Security Agency, *"if a ballot has issues that impacts its ability to be scanned, it can be hand counted."* The Maricopa County Board of Supervisors assured voters that *"sharpies do not invalidate ballots."* Dominion has stated that *"Sharpie pens are safe and reliable to use on ballots, and recommended due to their quick-drying ink."*

DOMINION VOTING

Founded in 2003, Dominion Voting Systems is a leading industry supplier of election technology across the U.S., Canada and globally.

PRODUCTS

EMS ENGINE
Democracy Suite®

IN-PERSON AND ACCESSIBLE VOTING
ImageCast® X

CENTRAL TABULATION
ImageCast® Central

COMBINATION VOTING AND TABULATION
ImageCast® Precinct
ImageCast® Evolution

Optional Solutions

ABOUT

Dominion Difference
Dominion Secure
Careers

INFO

Customer Support

1-866-654-VOTE (8683)

Contact Us

U.S.: Denver, CO

CANADA: Toronto, ON