AGENDA MATERIAL
DATE 5-3-22 ITEM NO. RA 17

Bernadette Russell

From: [redacted]
Sent: Sunday, May 1, 2022 12:03 AM
To: District1; DIST2; District3; District4; District5; COB_mail
Subject: May 3, 2022 agenda item

MAY 02'22 AM07:48 PC CLK OF BD

CAUTION: This message and sender come from outside Pima County. If you did not expect this message, proceed with caution. Verify the sender's identity before performing any action, such as clicking on a link or opening an attachment.

Please read these comments into records.

In Wisconsin, the Office of Special Counsel (OSC), headed by retired state Supreme Court Justice Michael Gableman, found that Dominion and ES&S voting machines were online and connected to the internet.

In Michigan, attorney and Secretary of State candidate, Matt Deperno, discovered a Telit LE910-SV1 modem chip embedded in the motherboard of an ES&S DS200 voting machine.
https://www.youtube.com/watch?v=Co91BdP_G_o

Through these modems, hackers could theoretically intercept results as they're transmitted on election night or, worse, use the modem connections to reach back into voting machines or the election management systems to install malware, change software, or alter official results. Therefore, not only are hackers able to penetrate elections through vulnerable USB cards and election management systems, but also through the very voting machines themselves.

This isn't a problem exclusive to elections, all computers are hackable, and that is why election security experts have always recommended hand-marked paper ballots and rigorous post-election audits.

This also isn't a partisan issue, both Democrats and Republicans are well aware of the secrecy, privatization, and hackable hardware and software that runs America's elections.

After the 2016 election, Clinton supporters and the corporate media would spend the next four years talking about how compromised America's computerized voting system was.

Senators Ron Wyden, Amy Klobuchar, and Kamala Harris held numerous congressional hearings where they explained that it was too easy to hack voting machines, too easy to find unattended voting machines and too many voting machines
were connected to the internet

Michael Aaron
Rita Ranch Resident

AGENDA MATERIAL
DATE 5-3-22 ITEM NO. RA 17

Bernadette Russell

From: [redacted]
Sent: Sunday, May 1, 2022 12:20 PM
To: COB_mail; District1; DIST2; District3; District4; District5
Subject: Addendum to the Agenda for the Board of Supervisors Meeting of Tuesday May 3, 2022.

I request the following comment becomes part of the Addendum to the Agenda for the Board of Supervisors Meeting of Tuesday, May 3, 2022.

Item 9 - Vote Center Implementation
This may be the most critical issue the Board of Supervisors is dealing with. Public trust in voting integrity is at a low. The majority of the population believes a photo ID is a valid requirement for voting.

Will voting centers be more secure than precinct polling places - my guess is not, let's hope I'm wrong. There are many questions begging an answer:
1) What is the cost comparison of the change to 129 voting centers from precinct polling places? What is the cost of the 40 intermittent employees being hired?
2) It is my understanding all drop boxes will have attendants and there will be no "large metal unattended boxes" used as drop boxes. Is this correct?
3) I understand E Poll books can read AZ drivers licenses. Does this mean all you need is a drivers license to vote?
4) What is the status of Vote Center security measures? How do we know machines are secure, votes are accurately recorded, etc.?
5) How are the voter roll records being cleaned up to accurately reflect Pima County voters? This last election mail-in ballots were sent to non residents who owned property in Pima County - what if they voted?
6) How are we interacting with tribal nations? What benefits are being provided?
7) How do we insure non-profit entities from other states, such as Center for Technology and Civic Life, are not providing funding for Pima county elections?

Most importantly, how are answers to questions like the above transmitted to the general public - certainly something that needs to happen before we institute Voting Centers - and insuring this information gets to voters is a primary responsibility of the Board of Supervisors.

Gail Ault
[redacted]
Pima County resident

AGENDA MATERIAL
DATE 5-3-22 ITEM NO. RA17

Bernadette Russell

From: [redacted]
Sent: Sunday, May 1, 2022 12:11 AM
To: District4; District1; DIST2; District3; District5; COB_mail
Subject: May 3, 2022 Comments AGAINST e-machines

MAY 02'22AM07:48 PC CLK OF BD

CAUTION: This message and sender come from outside Pima County. If you did not expect this message, proceed with caution. Verify the sender's identity before performing any action, such as clicking on a link or opening an attachment.

Read and add our comment into official records.

Democrats On Voting Machines

After the 2020 election, Trump supporters were censored and de-platformed even banned for pointing out the very same
vulnerabilities that Democrats and the corporate media had spent the last four years discussing. Regardless of politics, these vulnerabilities are very real, they still exist today, and they are best explained by the computer scientists who have spent the last two decades researching them.

Professor Matt Blaze, Georgetown University, Computer Science:
"I come here today as a computer scientist who spent the better part of the last quarter century studying election system security...
To be blunt, it's a widely recognized really indisputable fact that every piece of computerized voting equipment in use at polling places
today can be easily compromised in ways that have the potential to disrupt election operations, compromise firmware and software,
and potentially alter vote tallies in the absence of other safeguards. This is partly a consequence of historically poor design and
implementation by equipment vendors but it's ultimately a reflection of the nature of complex software. It's simply beyond the state
of the art to build software systems that can reliably withstand targeted attacks by a determined adversary in this kind of an environment...
Just as we don't expect the local sheriff to singlehandedly defend against military ground invasions, we shouldn't expect county election
IT managers to defend against cyber-attacks by foreign intelligence services."

Professor J. Alex Halderman, University of Michigan, Computer Science:
"I'm a professor of computer science and have spent the last ten years studying the electronic voting systems that our nation relies on.
My conclusion from that work is that our highly computerized election infrastructure is vulnerable to sabotage and even to cyber-attacks
that could change votes... I know America's voting machines are vulnerable because my colleagues and I have hacked them repeatedly
as part of a decade of research studying the technology that operates elections and learning how to make it stronger. We've created

attacks that can spread from machine to machine like a computer virus and silently change election outcomes. We've studied touch screen
and optical scan systems and in every single case we've found ways for attackers to sabotage machine and to steal votes...In close elections,
an attacker can probe the most important swing states or swing counties, find areas with the weakest protection, and strike there. In a close
election year, changing a few votes in key localities could be enough to tip national results."

Professor Andrew Appel, Princeton University, Computer Science:
"Installing new software is how you hack a voting machine to cheat. In 2009, in a courtroom of the superior court of New Jersey, I demonstrated
how to hack a voting machine. I wrote a vote-stealing computer program that shifted votes from one candidate to another. Installing that vote
stealing program in a voting machine takes seven minutes per machine with a screwdriver. But really the software I built was not rocket science.
Any computer programmer could write the same code. Once it's installed, it could steal elections without detection for years to come.
Other computer scientists have demonstrated similar hacks on many models of machine. This is not just one glitch from one manufacturer of machine,
it's the very nature of computers. So how can we trust our elections when it is so easy to make the computers cheat?"

Michael & Gisela Aaron
Rita Ranch Residents

Bernadette Russell

From: [redacted]
Sent: Sunday, May 1, 2022 12:00 AM
To: District1; DIST2; District3; District4; District5; COB_mail
Subject: May 3, 2022 Comments -AGAINST E-poll books

Comments for the record. WHY VOTERS DO NOT SUPPORT E-Poll Books nor any electronic devices!

Elections Systems & Software, Dominion Voting, and Hart Intercivic account for about ninety percent of U.S. election equipment.
These vendors supply the equipment of America's elections:

• Electronic Poll Books: An electronic poll book (also called "e-poll book") is a computer-based system that allows poll workers to look up voters
and either check them in to vote or identify the person as not in the list of voters permitted to vote at the polling location.

• Optical Scanners: Optical scanners include both marksense and digital image scanners in which voters mark paper ballots that are subsequently
tabulated by scanning devices. Optical scan voting systems can scan and tabulate ballots marked by hand or those marked by a ballot marking device.
High-capacity batch-fed optical scan tabulators are used in some jurisdictions to handle larger volumes of central count ballots.

• Direct Recording Electronic (DRE): A direct recording electronic voting system (often touchscreen) is a vote-capture device that allows the electronic
presentation of a ballot, electronic selection of valid contest options, and the electronic storage of contest selections as individual records. The voter's
choices are stored in DREs via a memory cartridge or smart card and added to the choices of all other voters.

• Ballot Marking Devices (BMD): A ballot marking device allows the electronic presentation of a ballot, electronic selection of valid contest options
and produces a machine-marked paper ballot, but does not make any other lasting record of the voter's selections.

• Hybrid Voting Systems: Hybrid voting systems combine elements of optical scanners, DREs, or ballot marking devices.

• Election Management System (EMS): A set of applications that handle pre- and post-voting activities, including ballot layout, programming media
for voting equipment, importing results data, and accumulating and reporting results. Contrary to popular belief, all electronic voting equipment can
be hacked because all such equipment must receive programming before each election from memory cards or USB drives prepared on election management

systems which are often computers not only connected to the internet but also running out-of-date versions of Windows. If a county election management
system is infected with malware, the malware can spread from that system to the USB drives, which then would transfer it to all the voting machines,
scanners, and ballot-marking devices in the county.

Gisela Aaron
Rita Ranch Resident

AGENDA MATERIAL
DATE 5-3-22 ITEM NO. RA 17

Bernadette Russell

From: [redacted]
Sent: Sunday, May 1, 2022 12:00 AM
To: District1; DIST2; District3; District4; District5; COB_mail
Subject: May 3, 2022 Agenda item 17/Addendum item 9

Please read our comments into records.

Your report for the May 3, 2022 meeting did not include any of our prior comments regarding E-polling centers, E-polling books and more.
Please include ALL comments AGAINST them. I will forward them in separate emails.

We do NOT support any electronic machines. They are hackable as touted by your fellow Democrats:
Let me refresh your memory... These statement can be easily verified on the Internet.

With both major parties doubting the integrity of the last two elections, the voting machine vendors have lost the trust of the American people. And, deservedly so.
Considering J.P. Morgan, Facebook, and the Pentagon have all been hacked in recent years, it is illogical to believe that voting machine manufacturers working on
limited budgets are somehow immune to cyber intrusions.

Senator Amy Klobuchar, D-Minn., discussed her concerns with the three main voting machine manufacturers in the 2020 HBO
Documentary, Kill Chain: The Cyber War on America's Elections: "We're very concerned because there are only three companies.
You could easily hack into them. It makes it seem like all these states are doing different things, but in fact, three companies are controlling them."

"Forty-three percent of American voters use voting machines that researchers have found have serious security flaws including backdoors.
These companies are accountable to no one. They won't answer basic questions about their cyber security practices and the biggest companies
won't answer any questions at all. Five states have no paper trail and that means there is no way to prove the numbers the voting machines put
out are legitimate. So much for cyber-security 101... The biggest seller of voting machines is doing something that violates cyber-security 101,
directing that you install remote-access software which would make a machine like that a magnet for fraudsters and hackers."

This statement was said by Senator Ron Wyden, D-Ore., during a March 21, 2018, U.S. Senate Intelligence Committee hearing, one of the numerous

hearings that Congress convened to discuss election security following the 2016 election. Wyden, his congressional colleagues, and the corporate media
would spend much of the next four years discussing their many concerns about the security of the U.S. election system.

Computerized voting in the United States is largely a secretive and privately-run affair conducted out of the public eye with very little oversight.
The corporations that run every aspect of America's elections, from voter registration to casting and counting votes, are subject to limited regulation and public scrutiny.
The companies are privately-owned, making information about ownership, finances, and technology difficult to obtain.
The software source code and hardware design are kept as trade secrets and therefore difficult to study or investigate.

Gisela Aaron
Rita Ranch resident

Bernadette Russell

From: [redacted]
Sent: Sunday, May 1, 2022 12:00 AM
To: District4; District1; DIST2; District3; District5; COB_mail
Subject: May 3, 2022 Agenda items

Please add these comments into records.

In 2008, the most serious breach in Pentagon history came from a single USB drive infected with a virus that spread swiftly
through the Defense Department's Secret Internet Protocol Router Network – the classified SIPRNet – as well as the Joint Worldwide Intelligence Communication System used by the U.S. government's top intel agencies.
After that hack, the Department of Defense severely restricted the use of USB drives, established programs to control and track personnel authorized to use them, and largely barred users by setting up computers without USB ports or restricting certain computer users to not recognize flash drives.

In contrast, the majority of the U.S. election system is programmed by local county election officials or third-party vendors,
who are plugging previously-used USB drives into computers connected to the internet, before plugging those same USB drives
into the optical scanners, tabulators, and voting machines that collect, count, and determine election results.

In 2019, the Associated Press reported that the vast majority of 10,000 election jurisdictions nationwide, including numerous
swing states, were still using Windows 7 or older operating systems to create ballots, program voting machines, tally votes, and report counts.
Windows 7 reached its "end of life" on Jan. 14, 2020, meaning Microsoft stopped providing technical support and producing "patches"
to fix software vulnerabilities. Furthermore, not only are U.S. elections being programmed on computers running out-of-date software,
but voting machine manufacturers have also installed remote-access software and wireless modems connecting voting machines directly to the internet.

NBC News reported ten months before the 2020 election that ES&S, the largest U.S. election machine vendor, had installed at least 14,000 modems
to connect their voting machines to the internet even though many election security experts had previously warned that voting machines with
modems were vulnerable to hackers: https://www.youtube.com/watch?v=KE4wj_Nylus

Dominion Voting Systems, the second-largest U.S. election machine vendor, which has given public presentations acknowledging their use

of modems in their voting machines, was also discovered to be running remote-access software during the 2020 election:
In Georgia, 20-year election worker, Susan Voyles, testified that Dominion Voting Systems employees "operated remotely" on her
ballot-marking devices and poll pads after the team experienced some technical problems with their machines.

Michael Aaron
Rita Ranch Resident

Bernadette Russell

From: [redacted]
Sent: Sunday, May 1, 2022 12:50 AM
To: District1; DIST2; District3; District4; District5; COB_mail
Subject: FW: February 15, 2022 Agenda Item Comments

Agenda items May 3, 2022 to be added to spreadsheet against e-poll books.

From [redacted]
Sent: Sunday, February 13, 2022 4:25 PM
To: District1 <District1@pima.gov>; DIST2 <DIST.2@pima.gov>; District3 <District.3@pima.gov>; District4 <District4@pima.gov>; District5 <District5@pima.gov>
Cc: COB_mail <COB_mail@pima.gov>
Subject: February 15, 2022 Agenda Item Comments

Pima County Board of Supervisors,

Electronic machines like e-poll books are prone to security breaches as exposed in multiple State elections. E-poll books contain voter registration databases and software that necessitate additional security protocols often dismissed by careless employees as seen in prior elections. Are e-poll books approved by our legislators? Why start a new process without proper voter in-put right before another election? E-poll books, wireless printers and tabulators are hackable. Having printers at the polling centers to print ballots does not provide secure chain of custody nor accurate accountability. How do you compare the number of registered voters to the number of printed ballots? You do NOT have my consent for e-poll books, unsecure paper, wireless printers, nor tabulator devices!

Regarding centralized polling centers, why would voters give up their neighborhood voting places where election workers would notice inconsistencies? Why reduce nearly 60% of polling locations to only 100? Why this mad dash to change things quickly? It will suppress voters. I cannot give my consent. We witnessed mass chaos and irregularities in the last presidential election that we cannot ever let happen again. I urge you to defeat these progressive recommendations that will forever change our country! We are witnessing illegals intentionally being brought into our country to change future voting outcomes. We are also seeing intentional obstructing of any Voter Integrity measures such as one election day, mail ballots for Military or invalids by request only, smaller but more precincts, voter roll maintenance, more oversight by observers, less technology and higher security, chain of custody, and no ballot harvesting. What are you doing to protect US?

Lastly, countries such as UK, Ireland, Denmark, Sweden, Norway, Switzerland, and Spain have no more COVID restrictions. It's time to end mask and vaccine harassments. End the State of Emergency because we have effective medicines now. Politicians caused this economic crisis with endless lockdowns and lawless mandates. Mandates are not laws. You do not have my consent to ever do this again.

Michael Aaron, Voter in Rita Ranch
Read my comments into your records.

AGENDA MATERIAL
DATE 5-3-22 ITEM NO. RA 17

Bernadette Russell

From: [redacted]
Sent: Sunday, May 1, 2022 12:57 AM
To: District1; DIST2; District3; District4; District5; COB_mail
Subject: FW: February 15th meeting comment

Add these comments into your spreadsheet for May 3, 2022 agenda.
These were not listed on your agenda item AGAINST e-voting machines.
Gisela Aaron, Tucson, AZ

From: [redacted]>
Sent: Friday, February 11, 2022 2:06 PM
To: District1 <District1@pima.gov>; DIST2 <DIST.2@pima.gov>; District3 <District.3@pima.gov>; District4 <District4@pima.gov>; District5 <District5@pima.gov>; COB_mail <COB_mail@pima.gov>
Subject: February 15th meeting comment

Pima County Board of Supervisors,

Please read my comments into records. Electronic voting machines pose a severe risk to the security and integrity of free and fair elections! We've seen the results of chaos that they have created in prior elections. Voters should reject the use of machines like computers or electronic poll books. Electronic poll books severely undermine election integrity as observed in the Georgia Election. Machines such as e-poll books are prone to malfunction, making it necessary to "adjudicate" voter intent. There were no safeguards, universal passwords were shared, unsecured back doors left the system vulnerable to hackers, and unsupervised adjudications far exceeded the norm of all prior elections in history. No machines!

In an interview with KVOA, "*Pima County Recorder Gabriella Cazares-Kelly wants Pima County voters to be able to vote at voting centers on Election Day rather than their specific polling place in their precinct.*" Why? "*She and Pima County interim Elections Director Mary Martinson introduced a proposal to the Pima County Election Integrity Commission to bring 100 vote centers to the county for Election Day voting... This will eliminate more than 200 individual polling places within precincts.*" Why eliminate 100 neighborhood polling places? That makes NO SENSE! In fact, we need more and smaller places closer to the voters. Her plan would alienate voters that have been going to the same familiar polling places for centuries.

"*Cazares-Kelly believes this will make voting faster, more convenient and ultimately increase turnout.*" Don't believe that! Centralized "voting centers" are being pushed by progressives to take over our elections. It would make it easier to cheat and easier to overwrite the will of the People. It's another ploy to take over the process so they can easier control the outcome and harness power to "fundamentally change" this country.

Please reject this Evil plan!

Gisela Aaron
Voter in Rita Ranch

Bernadette Russell

From: [redacted]
Sent: Sunday, May 1, 2022 12:47 AM
To: District1; DIST2; District3; District4; District5; COB_mail
Subject: FW: 3/1/22 Agenda Addendum Reconsideration of Authorization of Vote Centers

RE VOTE CENTERS
These earlier comments were not listed on your spreadsheet for agenda May 3, 2022.
Please add these or be accused of manipulating the public! Thanks.

From: [redacted]
Sent: Sunday, February 27, 2022 11:27 PM
To: district1@pima.gov; district2@pima.gov; district3@pima.gov; district4@pima.gov; district5@pima.gov; COB_mail@pima.gov
Subject: 3/1/22 Agenda Addendum Reconsideration of Authorization of Vote Centers

Re: 3/1/22 Agenda Addendum Reconsideration of Authorization of Vote Centers

Pima County Board of Supervisors,

Again, we urgently request please do NOT authorize centralized vote centers.
Consider, this would brutally eliminate more than 200 individual polling places within precincts!
It would reduce polling places to only 100. This irrational move makes no sense for the population you claim to serve.
Why disenfranchise voters by severely reducing access to familiar neighborhood polling locations?

Why should voters give up their neighborhood voting places where election workers would notice voting inconsistencies?
How will voters find these elusive vote centers? How will they get there, having to travel further? Imaging standing in line
for many hours in our summer heat to cast a vote and then patiently waiting for the ballot print outs. Vote centers and e-poll books
did not work well in Maricopa County. Election day turned into Election week, then Election month. What a disaster!

Remember senior election staff will be leaving. Do you trust newly hired staff in the Pima County election office to pull it off successfully?
You may be blamed too if things go wrong. You appear to blindly approve any wish list by staff. You should be pleasing voters not the staff.

What are you doing to protect voters? Reducing voting places will only suppress voter engagement. We cannot give our consent.

Have voters even been given a chance for input during public events? The sudden move toward electronic centralization of the voting process is highly suspect.
We do not trust it! The decision should be a non-partisan and is of great concern to the community regardless of political party.

Recall there was mass chaos and many irregularities in the last presidential election that we cannot ever let happen again. We urge you to champion voters.
We only ask for elections to be kept the same way they used to be conducted: one election day, one vote-one person, voter ID, mail ballots for
Military or invalids by request only, voter roll maintenance, oversight by observers, chain of custody, no ballot harvesting, less technology
but higher security, and importantly smaller but more precincts close to voters. Audits as prescribed by law.

Please champion Pima County voters. Thank you.

Gisela & Mike Aaron, Voters in Rita Ranch.
Please add our comments into official records.

Bernadette Russell

From: [redacted]
Sent: Sunday, May 1, 2022 12:42 AM
To: COB_mail; District1; DIST2; District3; District4; District5
Subject: FW: 3/1/22 Addendum Item, re Tenex Software Solutions Contract

These Comments below were NOT LISTED on your spreadsheet AGAINST e-pollbooks,

Nor Software TENEX warning, DO ADD them. Thank you.

From: [redacted]>
Sent: Sunday, February 27, 2022 1:22 PM
To: COB_mail@pima.gov; district1@pima.gov; district2@pima.gov; district3@pima.gov; district4@pima.gov; district5@pima.gov
Subject: 3/1/22 Addendum Item, re Tenex Software Solutions Contract

Gisela & Mike Aaron, Voters in Rita Ranch. Please add our comments into official records.

3/1/22 Addendum Item: Vote "NO" to Tenex Software Solutions Contract

Pima County Board of Supervisors,

We urge you to NOT approve the $1.5 million contract with Tenex Software Solutions. Why?

1. Uninterrupted Internet connection during Election Day is necessary for the e-poll books to function well. This is of great concern to us. Can you guarantee that internet connectivity will be secure in rural areas, within the Tucson metro area, or on tribal lands? We greatly doubt it.

2. Voters don't trust the e-poll books and Tenex software. We are concerned with Internet security, with the inexperienced new staff using them, and concerned that they receive sufficient and appropriate training. It would make it more difficult to observe when shenanigans are happening. Just look at the last election and the chaos those e-poll books caused in Maricopa County. E-poll books caused for an election day to last an entire week or was it a month? Do not approve this costly, hackable, and very unreliable electronic system.

3. Senior leadership in the Pima County Elections division are retiring. This system requires an experienced staff to implement the change without errors. Using the 2022 election as a practice run is unacceptable with so many vital statewide positions at stake. It is irresponsible during a time when Pima County's elections top management are in transition. What is the hurry to install the Tenex Software Solutions?

4. Did Procurement staff provide a detailed analysis of cost savings, if any, of e-poll books and "voting centers" versus precincts with paper polling books? The analysis should include total annual costs for all electronic and software used during elections including voting machines and software. Does the expanding annual cost for voting machines and software exceed the cost of a paper-based system of paper ballots, paper polling books or machine-/and hand counts to certify election results? Did Procurement staff demonstrate due diligence that they have done said detailed analysis, before requesting $1.5 million in expenditures for cloud-based solutions?

5. Have voters been given a chance for input during public events? The sudden move toward electronic centralization of the voting process is highly suspect. We do not trust it! The decision should be a non-partisan and is of great concern to the community regardless of political party.

6. A quick Internet search revealed a Security Warning for their website! https://www.tenexsolutions.com/about.html

Warning: Potential Security Risk Ahead

Firefox detected an issue and did not continue to www.tenexsolutions.com. The website is misconfigured. It's likely the website's certificate is expired, which prevents Firefox from connecting securely. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details. What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it. You can notify the website's administrator about the problem.

To top it off, we found there is a sister company of Tenex Software Solutions based in RUSSIA!

At a time when voters distrust those electronic systems, it is reprehensible to even suggest purchasing them!

We insist on old fashioned, reliable paper rolls. Secure paper ballots with multiple security provisions. Limited paper at small polling places near voters. Chain of custody for the secure paper! Chain of custody for every step of the way. Access of observers. Oversight by both parties. One day election day. Voter ID. Voting for American or Naturalized citizens only! Limited ballots mailed to military and by request only.

Voters demand AUDITS for every election from now on. This is our right as provided by the law.

AGENDA MATERIAL
DATE 5-3-22 ITEM NO. RA 17

Bernadette Russell

From: [redacted]
Sent: Sunday, May 1, 2022 12:17 AM
To: District4; District1; DIST2; District3; District5; COB_mail
Subject: 5/3/20222 Comment against e-poll books (1-25)

Add comments to spreadsheet AGAINST E-poll books.

The bedrock of our Constitutional Republic is free and fair elections.
These articles can be easily found on-line. They are in order by years.

1. NYT: How to Hack an Election (Jan. 31, 2004)
2. CNN: The trouble with e-voting (Aug. 30, 2004)
3. Princeton: Security Analysis of the Diebold Accuvote-TS Voting Machine (Sept. 13, 2006)
4. TechReview: How to Hack an Election in One Minute (Sept. 18, 2006)
5. CNN: Dobbs: Voting Machines Put U.S. Democracy At Risk (Sept. 21, 2006)
6. HBO: Hacking Democracy (Nov. 2, 2006)
7. Salon: Hacking Democracy (Nov. 2, 2006)
8. NYT: Scientists' Tests Hack Into Electronic Voting Machines in California and Elsewhere (July 28, 2007)
9. Wired: Whistleblower: Voting Machine Company Lied to Election Officials About Reliability of Machines (March 27, 2008)
10. CNN: Computerized Systems Also Vulnerable To Hacking (Oct. 30, 2008)
11. Wired: ES&S Voting Machines Can Be Maliciously Calibrated to Favor Specific Candidates (Nov. 3, 2008)
12. CNN: Hacking Your Vote (Oct. 27, 2010)
13. TechReview: How Long Before Hackers Steal Votes? (March 18, 2011)
14. NBC: It only takes $26 to hack a voting machine (Sept. 28, 2011)
15. PBS: Internet Voting: Will Democracy or Hackers Win? (Feb. 16, 2012)
16. WSJ: Will The Next Election Be Hacked? (Aug. 17, 2012)
17. PopSci: How I Hacked An Electronic Voting Machine (Nov. 5, 2012)
18. Verge: Feed the machine: America's stumble through a decade of electronic voting (Nov. 6, 2012)
19. BrennanCenter: America's Voting Machines At Risk (Sept. 15, 2014)
20. Guardian: Voting machine password hacks as easy as 'abcde' (April 15, 2015)
21. NYT: Millions of Voter Records Posted, and Some Fear Hacker Field Day (Dec. 30, 2015)
22. Politico: More than 20 states have faced major election hacking attempts, DHS says (Sept. 30, 2016)
23. Wired: America's Electronic Voting Machines Are Scarily Easy Targets (Aug. 2, 2016)
24. Politico: How to Hack an Election in 7 Minutes (Aug. 5, 2016)
25. LawfareBlog: Secure the Vote Today (Aug. 8, 2016)

Michael & Gisela Aaron
Rita Ranch Residents

Bernadette Russell

From: [redacted]
Sent: Sunday, May 1, 2022 12:25 AM
To: District4; District1; DIST2; District3; District5; COB_mail
Subject: 5/30/2022 Agenda Items (26-50)

Please add these news articles (to your spreadsheet, AGAINST machines) that depict the dangers of election machines, their vulnerabilities and their threat to a free society, as illustrated in the last election.

26. CNN: Just How Secure Are Electronic Voting Machines? (Aug. 9, 2016)
27. CBS: Hacker demonstrates how voting machines can be compromised (Aug. 10, 2016)
28. ABC: Yes, It's Possible to Hack the Election (Aug. 19, 2016)
29. Atlantic: How Electronic Voting Could Undermine the Election (Aug. 29, 2016)
30. FOX: Princeton Professor demonstrates how to hack a voting machine (Sept. 18, 2016)
31. Fortune: Watch This Security Researcher Hack a Voting Machine (Nov. 4, 2016)
32. Vox: Here's how hackers can wreak havoc on Election Day (Nov. 7, 2016)
33. PBS: Here's how hackers might mess with electronic voting on Election Day (Nov. 8, 2016)
34. Slate: Now Is the Time to Replace Our Decrepit Voting Machines (Nov. 17, 2016)
35. PBS: Recounts or no, U.S. elections are still vulnerable to hacking (Dec. 26, 2016)
36. Politico: U.S. elections are more vulnerable than ever to hacking (Dec. 29, 2016)
37. ScientificAmerican: Our Voting System Is Hackable by Foreign Powers (March 1, 2017)
38. Politico: Will the Georgia Special Election Get Hacked? (June 14, 2017)
39. NPR: If Voting Machines Were Hacked, Would Anyone Know? (June 14, 2017)
40. HuffPost: Good News For Russia: 15 States Use Easily Hackable Voting Machines (July 17, 2017)
41. Forbes: These Hackers Reveal How Easy It Is To Hack US Voting Machines (July 29, 2017)
42. CNET: Defcon hackers find it's very easy to break voting machines (July 30, 2017)
43. CNN: We watched hackers break into voting machines (Aug. 11, 2017)
44. Intercept: The U.S. Election System Remains Deeply Vulnerable (Oct. 3, 2017)
45. NYT: The Myth of the Hacker-Proof Voting Machine (Feb. 2, 2018)
46. Slate: America's Voting Systems Are Highly Vulnerable to Hackers (Feb. 22, 2018)
47. NYT: I Hacked an Election. So Can the Russians. (April 5, 2018)
48. NewYorker: America Continues To Ignore Risks of Election Hacking (April 18, 2018)
49. Reuters: Old voting machines stir concerns among U.S. officials (May 31, 2018)
50. Axios: There's more than one way to hack an election (July 3, 2018)

Michael & Gisela Aaron
Rita Ranch Residents

Bernadette Russell

From: [redacted]
Sent: Sunday, May 1, 2022 12:29 AM
To: District4; District1; DIST2; District3; District5; COB_mail
Subject: 05/03/2022 Agenda items, add to your spreadsheet (51-75)

Comment for records.
Please add these news articles from 2018 to 2019 into your spreadsheet, AGAINST electronic voting machines:

51. Newsweek: Election Hacking: Voting-Machine Supplier Admits It Used Hackable Software Despite Past Denials (July 17, 2018)
52. Salon: Remote-access allowed: Voting machine company admits installing vulnerable software (July 20, 2018)
53. BBC: Hacking the US midterms? It's child's play (Aug. 11, 2018)
54. PBS: An 11-year-old changed election results on a replica Florida state website in under 10 minutes (Aug. 12, 2018)
55. Guardian: Why US elections remain 'dangerously vulnerable' to cyber-attacks (Aug. 13, 2018)
56. Guardian: Kids at hacking conference show how easily US elections could be sabotaged (Aug. 22, 2018)
57. National Academies of Sciences, Engineering, Medicine: Securing The Vote (Sept. 6, 2018)
58. CBS: Why voting machines in the U.S. are easy targets for hackers (Sept. 19, 2018)
59. NYT: The Crisis of Election Security (Sept. 26, 2018)
60. Politico: Attack on commonly used voting machine could tip an election (Sept. 27, 2018)
61. WSJ: Voting Machine Used in Half of U.S. Is Vulnerable to Attack (Sept. 27, 2018)
62. CNN: Hackers Bring Stark Warning About Election Security (Sept. 27, 2018)
63. Wired: Voting Machines Are Still Absurdly Vulnerable to Attacks (Sept. 28, 2018)
64. JenniferCohn: The genesis of America's corrupted computerized election system (Oct. 10, 2018)
65. Slate: Can Paper Ballots Save Our Democracy? (Oct. 10, 2018)
66. NYT: America's Elections Could Be Hacked. Go Vote Anyway (Oct. 19, 2018)
67. Vox: The hacking threat to the midterms is huge. (Oct. 25, 2018)
68. Forbes: Threats Obvious, But Electronic Voter Systems Remain Insecure (Nov. 1, 2018)
69. SciAmerican: The Vulnerabilities of Our Voting Machines (Nov. 1, 2018)
70. NYT: The Election Has Already Been Hacked (Nov. 3, 2018)
71. NYBooks: Voting Machines: What Could Possibly Go Wrong? (Nov. 5, 2018)
72. GQ: How to Hack an Election (Nov. 5, 2018)
73. Salon: Philly ignores cybersecurity and disability access in voting system selection (Feb. 16, 2019)
74. Politico: State election officials opt for 2020 voting machines vulnerable to hacking (March 1, 2019)
75. TechCrunch: Senators demand to know why election vendors still sell voting machines with 'known vulnerabilities' (March 27, 2019)

Michael & Gisela Aaron
Rita Ranch Residents

AGENDA MATERIAL
DATE 5-3-22 ITEM NO. RA 17

Bernadette Russell

From: [redacted]
Sent: Sunday, May 1, 2022 12:34 AM
To: District1; DIST2; District3; District4; District5; COB_mail
Subject: 05/03/22 Agenda Items - add to spreadsheet

CAUTION: This message and sender come from outside Pima County. If you did not expect this message, proceed with caution. Verify the sender's identity before performing any action, such as clicking on a link or opening an attachment.

MAY 02'22AM07:49 RCVD CLK OF BD

Read into records.

Please add these articles (2019-2020) 75-99 to your spreadsheet, AGAINST voting machines

75. Salon: New "hybrid" voting system can change paper ballot after it's been cast (March 28, 2019)
76. AP: Exclusive: New Election systems use vulnerable software (July 13, 2019)
77. Vice: Critical US Election Systems Have Been Left Exposed Online (Aug. 8, 2019)
78. CNN: Watch this hacker break into a voting machine (Aug. 10, 2019)
79. NBC: How Hackers Can Target Voting Machines (Aug. 12, 2019)
80. WaPo: Hackers were told to break into U.S. voting machines. They didn't have much trouble. (Aug. 12, 2019)
81. MITTech: 16 million Americans will vote on hackable paperless machines (Aug. 13, 2019)
82. Salon: Hackers can easily break into voting machines used across the US (Aug. 14, 2019)
83. FOX: Election machine keys are on the Internet, hackers say (Aug. 22, 2019)
84. Hill: Voting machines pose a greater threat to our elections than foreign agents (Oct. 2, 2019)
85. NPR: Cyber Experts Warn Of Vulnerabilities Facing 2020 Election Machines (Sept. 4, 2019)
86. JenniferCohn: America's Electronic Voting System is Corrupted to the Core (Sept. 7, 2019)
87. Wired: Some Voting Machines Still Have Decade-Old Vulnerabilities (Sept. 26, 2019)
88. Hill: Hacker conference report details persistent vulnerabilities to US voting systems (Sept. 26, 2019)
89. MotherJones: Researchers Assembled over 100 Voting Machines. Hackers Broke Into Every Single One. (Sept. 27, 2019)
90. WaPo: The Cybersecurity 202: U.S. voting machines vulnerable to hacks in 2020, researchers find (Sept. 27, 2019)
91. RollingStone: John Oliver Breaks Down Faulty Election Machine Security on 'Last Week Tonight' (Nov. 4, 2019)
92. Bloomberg: Expensive, Glitchy Voting Machines Expose 2020 Hacking Risks (Nov. 8, 2019)
93. NYBooks: How New Voting Machines Could Hack Our Democracy (Dec. 17, 2019)
94. WaPo: Voting machines touted as secure option are actually vulnerable to hacking, study finds (Jan. 8, 2020)
95. NBC: 'Online and vulnerable': Experts find nearly three dozens U.S. voting systems connected to internet (Jan. 10, 2020)
96. ElectionLawJournal: Ballot-Marking Devices (BMDs) Cannot Assure the Will of the Voters (Feb. 14, 2020)
97. AP: Reliability of pricey new voting machines questioned (Feb. 23, 2020)
98. Guardian: Hack the vote: terrifying film shows how vulnerable US elections are (March 26, 2020)

Michael & Gisela Aaron
Rita Ranch Residents

Bernadette Russell

From: [redacted]
Sent: Sunday, May 1, 2022 12:38 AM
To: District4; District1; DIST2; District3; District5; COB_mail
Subject: 05/03/2022 Agenda item spreadsheet

Please add these comments into records. Add to your agenda item spreadsheet **against** e-poll books.

100. HBO: Kill Chain: The Cyber War on America's Elections (March 26, 2020)
101. WSJ: Why a Data-Security Expert Fears U.S. Voting Will Be Hacked (April 24, 2020)
102. WhoWhatWhy: Touchscreen Voting Machines And The Vanishing Black Votes (May 27, 2020)
103. KimZetter: The Election Security Crisis and Solutions for Mending It (Sept.1, 2020)
104. DotLA: LA County is Tabulating Votes with QR Codes. Security Experts Think It's a Bad Idea (Oct. 22, 2020)
105. AJC: In high-stakes election, Georgia's voting system vulnerable to cyberattack (Oct. 23, 2020)
106. NYBooks: How Safe Is the US Election From Hacking? (Oct. 31, 2020)
107. USA Today: Will your ballot be safe? Computer experts sound warnings on America's voting machines (Nov. 2, 2020)
108. Politico: One big flaw in how Americans run elections (Nov. 2, 2020)
109. HeritageFoundation: Iranian Hackers Indictment Shows Vulnerability of Online Voter Registration (Nov. 30, 2021)
110. GovernmentTechnology: Report: Hackers Can Flip Votes in Georgia's Voting System (Jan. 27, 2022)

Michael & Gisela Aaron
Rita Ranch Residents

AGENDA MATERIAL
DATE 5-3-22 ITEM NO. RA 17

Bernadette Russell

From: Grace Stambaugh <[redacted]>
Sent: Monday, May 2, 2022 7:08 AM
To: District5; COB_mail; District1; DIST2; District3; District4
Subject: voting centers in Pima County - Agenda item 17/Addendum item 9 of concern

Pima County is reducing the number of voting locations to just over 100 for the entire county and then going to proceed using federally uncertified Electronic Poll Books (i.e., electronic Apple tablets connected to the internet), and change the rules of operation of the polling locations a months before the Primary Elections and just four months before the 2022 General Election! Research shows consolidating polling places suppresses voter turnout. This is particularly true for minority and low-income voters. Electronic Poll Books invite hackers and deceptive activities.
Pima County Elections and Recorder want to turn over the security of Pima County elections to third party vendors like Amazon Web Services, Cisco, and Tenex Software Solutions. Really, after what happened in 2020?

Why is any county doing this? Paper ballots is the only way to handle this upcoming election. **Please make sure you have sufficient budget for an audit of the upcoming election results.**

Grace Stambaugh

Bernadette Russell

From: S. Fickes <[redacted]>
Sent: Monday, May 2, 2022 8:58 AM
To: COB_mail; District1; DIST2; District3; District4; District5
Subject: BOS Meeting 05-03-22 Agenda Comments

I am Sharon Fickes, legal resident of Green Valley, AZ. Contact [redacted]
Following are my comments for the Board of Supervisors' meeting May 5, 2022

Agenda #17 Vote Centers and Addendum #9 Vote Center Implementation
Pima County registered voters based on Redistricting Data & Map information for Map Option 2b.2a total 626,915 potential voters. They will now no longer go to their local Precinct but instead choose from 129 Vote Centers (606 potential voters per center/8 hour average) . Fingers crossed our Pima County voters are not confused or overwhelmed by this new system. In a January 20, 2022 memo from Jan Lesher to the Board of Supervisors in her support of the Vote Centers, she mentions some of the benefits are: fewer provisional ballots. Contrary to the Elections Department Additional Information from Constance Hargrove, Elections Director, where she enumerates the Elections Department back-up plan is to use provisional ballots for problems at Vote Center. Also back-up paper ballots and that voting equipment specialists will be assigned to each Vote Center. Well what happens to the connections that are lost at these Vote Centers and voters stand around waiting to proceed? Who is going to fix that issue? Please discuss, in-depth, these issues and more with Constance Hargrove, Pima County new Elections Director. She was in the middle of a similar mess when she was the responsible individual in Virginia during the 2020 election cycle.