Subject: FW: Response to 2024-06-27 American Oversight to Multiple PRR
Date: Wednesday, September 18, 2024 at 9:00:20 AM Eastern Daylight Time
From: Ben Sparks
To: AO Records
Attachments: image001.png, Rep 91 (Rep91@ohiohouse.gov).pdf, Rep. Bob Peterson (Bob.Peterson@ohiohouse.gov).pdf, Riley Eberhart (Riley.Eberhart@ohiohouse.gov).pdf, Rep 74 (Rep74@ohiohouse.gov).pdf, Rep. Bernie Willis (Bernard.Willis@ohiohouse.gov).pdf, Logan Hannum (Logan.Hannum@ohiohouse.gov).pdf

Good morning!

The below email and attached documents are ready for processing in response to OH-REP-24-1295 and OH-REP-24-1296. If you have any questions, just let me know!

Thanks!

Ben

--
Ben Sparks | he/him/his
Senior Counsel | American Oversight
ben.sparks@americanoversight.org | (202) 873-1741
www.americanoversight.org | @weareoversight

From: McGuire, Mike <Mike.McGuire@ohiohouse.gov>
Date: Tuesday, September 17, 2024 at 4:27 PM
To: Ben Sparks <ben.sparks@americanoversight.org>, AO Records <records@americanoversight.org>
Cc: Blessing, Heather <Heather.Blessing@ohiohouse.gov>, Austin, Bryanna <Bryanna.Austin@ohiohouse.gov>
Subject: Response to 2024-06-27 American Oversight to Multiple PRR

To: records@americanoversight.org and ben.sparks@americanoversight.org

Good afternoon:

This email responds to your revised public records request dated June 27, 2024, in which you requested the following:

All email communications (including emails, email attachments, complete email chains, calendar invitations, and calendar invitation attachments) during the period from February 1, 2024, through June 27, 2024, between Representative Bob Peterson or his Legislative Aide, Riley Eberhart, or Representative Bernard Willis or his Legislative Aide, Logan Hannum the named individuals:

1. Cleta Mitchell;
2. Doug Frank;
3. James Rigano;
4. Marius Paulikas;
5. Mike Lindell;
6. Gina Swoboda;
7. Mark Cook;
8. Jason Snead;
9. Marcell Strbich;
10. Derek Lyons;
11. Kerri Toloczko;
12. Hans van Spakovsky;
13. J. Kenneth Blackwell

Regarding House Bill 472 and the identified related terms (i.e., “election integrity”, “election systems”, “hand count”, “manual count”, “Ohioans for Transparency”, “provisional ballot”, “tabulating equipment”, “tabulation equipment”, “voter registration data”, “votes count”, “voting machine”, “voting systems”, “hand-count”, or “handcount”, “OEIN”, “Ohio EIN”, “America First Policy Institute”, “Election Integrity Network”, “whoscounting”, “Hand County Road Show”, “Honest Elections Project”, “Heritage Foundation”, “heritageaction”, and/or “Ohio Votes Count”).

I have interpreted your request for public records to apply to General Correspondence (House-General 12) under the House Records Retention Schedule.

Please find attached all responsive records. No records have been withheld.

With this email, we conclude our response and close our file on your request.

Sincerely,

Mike McGuire

Mike McGuire
Sr. Deputy Legal Counsel, Majority Caucus
Ohio House of Representatives
77 S. High Street Columbus,
14th Floor, Ohio 43215
Office: (614) 466-8118 / Cell: (330) 814-2780

Hannum, Logan

From: Willis, Bernard
Sent: Monday, March 25, 2024 4:13 PM
To: mstrbic
Cc: Gail Niederlehner; Jim Rigano; swiggam@gmail.com; Hannum, Logan; Peterson, Bob
Subject: Re: Buckeye Institute Introduction to Ohio Election Bill

I love it. Let's get together with them soon. Maybe we can set up a F2F meet after Easter?

Bunyan

Get Outlook for iOS

From: mstrbic <mstrbic@protonmail.com>
Sent: Sunday, March 24, 2024 10:19 PM
To: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Cc: Gail Niederlehner <ohio4truth@proton.me>; Jim Rigano <jim@rigano.net>; swiggam@gmail.com <swiggam@gmail.com>
Subject: Fw: Buckeye Institute Introduction to Ohio Election Bill

Representative Willis,

Senior Legal Fellow of Conservative Partnership Institute (CPI) Cleta Micthell has come out strong for the proposed Ohio Votes Count Act. She offered to broker an introduction to the Buckeye Institute President Robert Alt for bill proponency.

Support of the election bill from the States foremost conservative affiliated think tank would lend further credibility to legislators considering co-sponsorship should they take a public position or testify on the bill.

Please feel free to share this development with the Committee Chairman.

Thank you,
Marcell Strbich
Ohio Elections Study Collaborative

Sent with Proton Mail secure email.

-------- Forwarded Message -------
From: mstrbic <mstrbic@protonmail.com>
Date: On Sunday, March 24th, 2024 at 11:55 PM
Subject: Buckeye Institute Introduction to Ohio Election Bill
To: Cleta Mitchell <cleta@cletamitchell.com>
CC: Bryson Davis <bryson@electionintegrity.network>, Eileen Watts <ewattsohio@gmail.com>, Jim Womack <james.k.womack@gmail.com>, Barry Chapman <bchapman@cox.net>, Gail Niederlehner <ohio4truth@proton.me>, Jim Rigano <jim@rigano.net>, Eileen Watts <ewatts@columbus.rr.com>, ws095@hotmail.com <ws095@hotmail.com>

Hi Cleta,

Great idea! Could you please broker an introduction to Robert Alt of the Buckeye Institute to myself, Eileen Watts, and former Ohio legislator advisor Bill Schuck? Would a conference call sometime this week be possible?

Our objectives for the meeting involve introducing the following-

- Highlights of OH's citizen-initiated pending election bill (Exec Summary Attached)
  - Existing OH voter registration verification and data validation deficiencies
  - Overview of voting system certification standards, State non-compliance & security deficiencies
- BMV disclosed findings on non-citizens possessing OH voter credentials (Attached)
- Pending SoS FOIA request for 2023 annual non-citizen audit results of Statewide Registration Database (Attached)

We really could benefit from partnering with the renowned Buckeye Institute for legal support, advise and advocacy in the coming weeks as multiple legislative and potential legal filings coalesce leading up to the 2024 election.

Thank you,
Marcell Strbich

Sent with Proton Mail secure email.

On Sunday, March 24th, 2024 at 7:15 AM, Cleta Mitchell <cleta@cletamitchell.com> wrote:

Oh wow! That's phenomenal!!

Your data about noncitizens - have you petitioned the SOS to remove those registrations specifically and submitted with documentation of noncitizen status?

Have you considered reaching out to Robert Alt at Buckeye Institute to represent the coalition and file suit to remove these and other new noncitizens asap?

I'd be happy to connect you with Robert. Let me know. Cleta

Cleta Mitchell, Esq.
Senior Legal Fellow
Conservative Partnership Institute

202.431.1950 (cell)
cleta@cletamitchell.com
www.whoscounting.us

On Mar 23, 2024, at 10:16 PM, mstrbic <mstrbic@protonmail.com> wrote:

Hi Cleta,

We'll definitely look to bring Ralph onboard. To answer your question, our efforts (OEIN) are independent of the United Sovereign Americans (USA); however, the provisions within our proposed election bill would solve many of the voter registration inaccuracies and subsequent registration and voting violations alleged in the complaint.

I've attached a 1-pg Executive Summary of a constituent written election bill that will drop in Ohio's House in early Apr. The Chairman of Government Oversight Accountability Committee Rep Bob Peterson agreed to co-sponsor with Rep Berni Willis. Both State House Speaker and Senate

President were apprised and receptive to bringing this election bill to a full vote in legislature when ready.

Of note, the bill proposes multiple 1st-in-the nation measures-

- State-directed independent 3rd party cyber security assessment reviews of voting systems as condition of certification in addition to EAC VVSG 2.0 standards

- Defined voting system certification standards based on most up to date federal software security development guidelines to include vendor voting system disclosure requirements

- Independent audits of Voter Registration Databases by Auditor of State

- Adoption of anti-tamper proof digital blockchain ledger functionality for Voter Registration Databases at both State and County level

- Voter registration data validation measures and identity and citizenship verification PRIOR to SoS acceptance on voter rolls (i.e. Not being done today – 267K+ illegals in Ohio)

- County opt-in provision for hand counted paper ballots in place of voting machines.

If you or other stakeholders are interested, we can provide a presentation.

Let me know.

Marcell Strbich
Ohio Election Research Collaborative (OEIN Affiliate)

Sent with Proton Mail secure email

Sent with Proton Mail secure email.

On Sunday, March 24th, 2024 at 7:15 AM, Cleta Mitchell <cleta@cletamitchell.com> wrote:

> Oh wow! That's phenomenal!!
>
> Your data about noncitizens - have you petitioned the SOS to remove those registrations specifically and submitted with documentation of noncitizen status?
>
> Have you considered reaching out to Robert Alt at Buckeye Institute to represent the coalition and file suit to remove these and other new noncitizens asap?
>
> I'd be happy to connect you with Robert. Let me know. Cleta
>
> Cleta Mitchell, Esq.
> Senior Legal Fellow
> Conservative Partnership Institute
>
> 202.431.1950 (cell)
> cleta@cletamitchell.com
> www.whoscounting.us

On Mar 23, 2024, at 10:16 PM, mstrbic <mstrbic@protonmail.com> wrote:

Hi Cleta,

We'll definitely look to bring Ralph onboard. To answer your question, our efforts (OEIN) are independent of the United Sovereign Americans (USA); however, the provisions within our proposed election bill would solve many of the voter registration inaccuracies and subsequent registration and voting violations alleged in the complaint.

I've attached a 1-pg Executive Summary of a constituent written election bill that will drop in Ohio's House in early Apr. The Chairman of Government Oversight Accountability Committee Rep Bob Peterson agreed to co-sponsor with Rep Berni Willis. Both State House Speaker and Senate President were apprised and receptive to bringing this election bill to a full vote in legislature when ready.

Of note, the bill proposes multiple 1st-in-the nation measures-

- State-directed independent 3rd party cyber security assessment reviews of voting systems as condition of certification in addition to EAC VVSG 2.0 standards

- Defined voting system certification standards based on most up to date federal software security development guidelines to include vendor voting system disclosure requirements

- Independent audits of Voter Registration Databases by Auditor of State

- Adoption of anti-tamper proof digital blockchain ledger functionality for Voter Registration Databases at both State and County level

- Voter registration data validation measures and identity and citizenship verification PRIOR to SoS acceptance on voter rolls (i.e. Not being done today – 267K+ illegals in Ohio)

- County opt-in provision for hand counted paper ballots in place of voting machines.

If you or other stakeholders are interested, we can provide a presentation.

Let me know.

Marcell Strbich
Ohio Election Research Collaborative (OEIN Affiliate)

Sent with Proton Mail secure email.

Hannum, Logan

Subject:	Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion
Location:	Microsoft Teams Meeting
Start:	Tue 6/4/2024 10:00 AM
End:	Tue 6/4/2024 10:30 AM
Recurrence:	(none)
Meeting Status:	Meeting organizer
Organizer:	Hannum, Logan
Required Attendees:	Willis, Bernard; dauren.h.mason.nfg@army.mil; mstrbic@protonmail.com; Eberhart, Riley
SkypeTeamsProperties:	{"cid":"19:meeting_ZTg5YWM4ZTMtYzhhYy00Y2RlLWJiZGUtMjczNTU0NTc5Yzkw@thread.v2","rid":"0","mid":"0","private":true,"type":0}
SkypeTeamsMeetingUrl:	https://teams.microsoft.com/l/meetup-join/19%3ameeting_ZTg5YWM4ZTMtYzhhYy00Y2RlLWJiZGUtMjczNTU0NTc5Yzkw%40thread.v2/0?context=%7b%22Tid%22%3a%225fbc1338-b4f6-4a8f-91a9-43523a0b679f%22%2c%22Oid%22%3a%226145e2d3-0c79-4374-b47f-385e1650b72a%22%7d
SchedulingServiceUpdateUrl:	https://api.scheduler.teams.microsoft.com/teams/5fbc1338-b4f6-4a8f-91a9-43523a0b679f/6145e2d3-0c79-4374-b47f-385e1650b72a/19_meeting_ZTg5YWM4ZTMtYzhhYy00Y2RlLWJiZGUtMjczNTU0NTc5Yzkw@thread.v2/0
TeamsVtcTenantId:	5fbc1338-b4f6-4a8f-91a9-43523a0b679f
MeetingTemplateId:	default

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 255 398 727 065

Passcode: 3ozsaJ

Dial in by phone

+1 380-215-0572,,308674113# United States, Columbus

Find a local number

Phone conference ID: 308 674 113#

For organizers: Meeting options | Reset dial-in PIN

Hannum, Logan

From: Willis, Bernard
Sent: Monday, June 3, 2024 9:26 AM
To: Hannum, Logan; Marcell mstrbic
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Oh yeah, you told me that.... Well I say keep it for tomorrow. I will try to join, but really need Marcell on that Teams meeting to talk about the Cyber

Bunyan

Get Outlook for iOS

From: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Sent: Monday, June 3, 2024 9:08:47 AM
To: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

The issue is, he's on military leave from the 7-23 so not much time in between.

Get Outlook for iOS

From: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Sent: Monday, June 3, 2024 8:39:47 AM
To: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Would have to push it to the following Monday if possible..

Get Outlook for iOS

From: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Sent: Monday, June 3, 2024 8:07:47 AM
To: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Subject: RE: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Is there a time that would work better for you that you could be able to make it? Either way, I do think it would be a good idea for him to be in attendance.

-----Original Appointment-----
From: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Sent: Friday, May 31, 2024 8:12 PM
To: Hannum, Logan
Subject: Tentative: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion
When: Tuesday, June 4, 2024 10:00 AM-10:30 AM (UTC-05:00) Eastern Time (US & Canada).
Where: Microsoft Teams Meeting

I can't even be on Teams at that time, but do you think I should have Chachi (Lt Col Retired Marcell Strbich) attend?

Hannum, Logan

From: mstrbic <mstrbic@protonmail.com>
Sent: Monday, June 3, 2024 1:40 PM
To: Hannum, Logan
Cc: Willis, Bernard
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Logan,

Please send me the zoom link and your contact info for Tomm's 1000 mtg. I can lead HB 472 cyber security overview provisions with Cyber Reserve Reps.

-Marcell Strbich
937-607-4237

On Mon, Jun 3, 2024 at 9:25 AM, Willis, Bernard <Bernard.Willis@ohiohouse.gov> wrote:

> Oh yeah, you told me that.... Well I say keep it for tomorrow. I will try to join, but really need Marcell on that Teams meeting to talk about the Cyber
>
> Bunyan
>
> Get Outlook for iOS
>
> ---
>
> **From:** Hannum, Logan <Logan.Hannum@ohiohouse.gov>
> **Sent:** Monday, June 3, 2024 9:08:47 AM
> **To:** Willis, Bernard <Bernard.Willis@ohiohouse.gov>
> **Subject:** Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion
>
> The issue is, he's on military leave from the 7-23 so not much time in between.
>
> Get Outlook for iOS
>
> ---
>
> **From:** Willis, Bernard <Bernard.Willis@ohiohouse.gov>
> **Sent:** Monday, June 3, 2024 8:39:47 AM
> **To:** Hannum, Logan <Logan.Hannum@ohiohouse.gov>
> **Subject:** Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion
>
> Would have to push it to the following Monday if possible..
>
> Get Outlook for iOS
>
> ---
>
> **From:** Hannum, Logan <Logan.Hannum@ohiohouse.gov>
> **Sent:** Monday, June 3, 2024 8:07:47 AM
> **To:** Willis, Bernard <Bernard.Willis@ohiohouse.gov>
> **Subject:** RE: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Is there a time that would work better for you that you could be able to make it? Either way, I do think it would be a good idea for him to be in attendance.

-----Original Appointment-----
From: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Sent: Friday, May 31, 2024 8:12 PM
To: Hannum, Logan
Subject: Tentative: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion
When: Tuesday, June 4, 2024 10:00 AM-10:30 AM (UTC-05:00) Eastern Time (US & Canada).
Where: Microsoft Teams Meeting

I can't even be on Teams at that time, but do you think I should have Chachi (Lt Col Retired Marcell Strbich) attend?

Hannum, Logan

From: Hannum, Logan
Sent: Monday, June 3, 2024 1:54 PM
To: mstrbic
Cc: Willis, Bernard
Subject: RE: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Afternoon Marcell:

This meeting should be rather small in size. This is a prep meeting with our TAG liaison to really engage on the Cyber Security side of the bill. I am excited you will be able to join and will send the Teams link over to you here very shortly!

S & B

Logan J. Hannum MPS
Legislative Aide
Representative Bernard "Bunyan" Willis
House District 74

From: mstrbic <mstrbic@protonmail.com>
Sent: Monday, June 3, 2024 1:40 PM
To: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Cc: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Logan,

Please send me the zoom link and your contact info for Tomm's 1000 mtg. I can lead HB 472 cyber security overview provisions with Cyber Reserve Reps.

-Marcell Strbich
937-607-4237

On Mon, Jun 3, 2024 at 9:25 AM, Willis, Bernard <Bernard.Willis@ohiohouse.gov> wrote:

> Oh yeah, you told me that.... Well I say keep it for tomorrow. I will try to join, but really need Marcell on that Teams meeting to talk about the Cyber
>
> Bunyan
>
> Get Outlook for iOS

From: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Sent: Monday, June 3, 2024 9:08:47 AM
To: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

The issue is, he's on military leave from the 7-23 so not much time in between.

Get Outlook for iOS

From: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Sent: Monday, June 3, 2024 8:39:47 AM
To: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Would have to push it to the following Monday if possible..

Get Outlook for iOS

From: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Sent: Monday, June 3, 2024 8:07:47 AM
To: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Subject: RE: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Is there a time that would work better for you that you could be able to make it? Either way, I do think it would be a good idea for him to be in attendance.

-----Original Appointment-----
From: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Sent: Friday, May 31, 2024 8:12 PM
To: Hannum, Logan
Subject: Tentative: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion
When: Tuesday, June 4, 2024 10:00 AM-10:30 AM (UTC-05:00) Eastern Time (US & Canada).
Where: Microsoft Teams Meeting

I can't even be on Teams at that time, but do you think I should have Chachi (Lt Col Retired Marcell Strbich) attend?

Hannum, Logan

From: Willis, Bernard
Sent: Tuesday, June 4, 2024 10:11 AM
To: Hannum, Logan; mstrbic
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

My meeting in TX is starting concurrently with this one now. I will be on just in case

Get Outlook for iOS

From: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Sent: Monday, June 3, 2024 12:54:00 PM
To: mstrbic <mstrbic@protonmail.com>
Cc: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Subject: RE: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Afternoon Marcell:

This meeting should be rather small in size. This is a prep meeting with our TAG liaison to really engage on the Cyber Security side of the bill. I am excited you will be able to join and will send the Teams link over to you here very shortly!

S & B

Logan J. Hannum MPS
Legislative Aide
Representative Bernard "Bunyan" Willis
House District 74

From: mstrbic <mstrbic@protonmail.com>
Sent: Monday, June 3, 2024 1:40 PM
To: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Cc: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Logan,

Please send me the zoom link and your contact info for Tomm's 1000 mtg. I can lead HB 472 cyber security overview provisions with Cyber Reserve Reps.

-Marcell Strbich
937-607-4237

On Mon, Jun 3, 2024 at 9:25 AM, Willis, Bernard <Bernard.Willis@ohiohouse.gov> wrote:

Oh yeah, you told me that.... Well I say keep it for tomorrow. I will try to join, but really need Marcell on that Teams meeting to talk about the Cyber

Bunyan

Get Outlook for iOS

From: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Sent: Monday, June 3, 2024 9:08:47 AM
To: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

The issue is, he's on military leave from the 7-23 so not much time in between.

Get Outlook for iOS

From: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Sent: Monday, June 3, 2024 8:39:47 AM
To: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Would have to push it to the following Monday if possible..

Get Outlook for iOS

From: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Sent: Monday, June 3, 2024 8:07:47 AM
To: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Subject: RE: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Is there a time that would work better for you that you could be able to make it? Either way, I do think it would be a good idea for him to be in attendance.

-----Original Appointment-----
From: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Sent: Friday, May 31, 2024 8:12 PM
To: Hannum, Logan
Subject: Tentative: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion
When: Tuesday, June 4, 2024 10:00 AM-10:30 AM (UTC-05:00) Eastern Time (US & Canada).
Where: Microsoft Teams Meeting

I can't even be on Teams at that time, but do you think I should have Chachi (Lt Col Retired Marcell Strbich) attend?

Hannum, Logan

From: mstrbic <mstrbic@protonmail.com>
Sent: Sunday, June 23, 2024 10:21 PM
To: Hannum, Logan; Rep Bernie Willis
Subject: HB 472 Presentation for OHCyR (Tues Mtg)
Attachments: Securing OHs Election Infrastructure_TAG Brief_ Jun 10 24.pptx

Logan

Please see attached presentation for this Tuesday's mtg with OHCyR. Let me know if you have any questions.

Thanks,
Marcell

Sent with Proton Mail secure email.

Securing Ohio's Election Infrastructure

Cybersecurity Primer – Legislation HB 472/SB 274

Ohio Election Study Collaborative

Presenter: Marcell Strbich, USAF, Lt Col (ret)

June 26thth 2024

The views expressed are those of the individual only and not those of the U.S. Air Force or Dept of Defense

AMERICAN OVERSIGHT

Overview

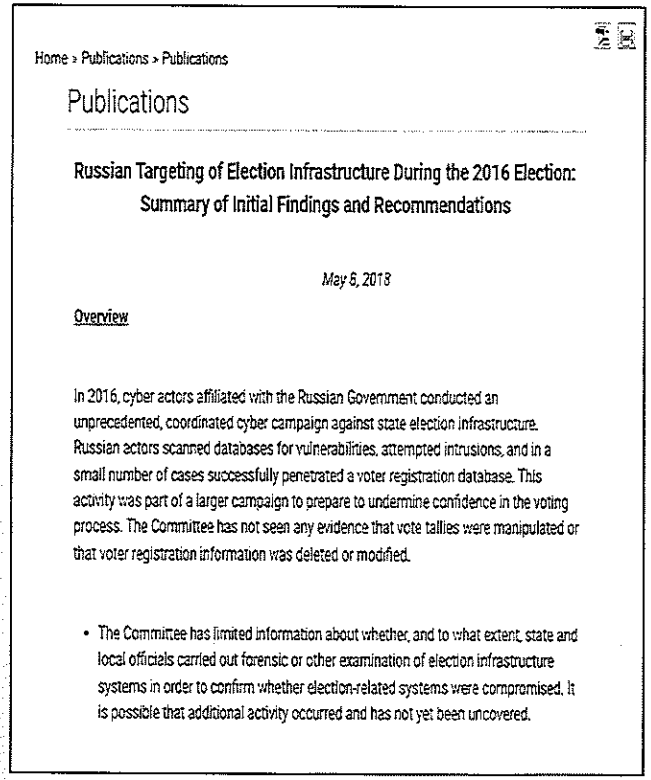
- Assessing Security Risk to Election Infrastructure
  - EO 14028 Improving the Nation's Cybersecurity
  - Election "Critical" Infrastructure Overview
  - Vendor – Products and Services Overview
- Federal Testing & Certification Process – The Problem
  - Voting System Certification – Issues & Challenges
  - Ohio Law Disconnect with Federal Law
- Voting System Certification Issues & Challenges
  - Cybersecurity Functions Framework
  - Wireless Network Configuration – Patent Example
  - Current Law Vs. Standard – Election Systems
- Current Ohio Election Security Measures – The Gap
  - Current Ohio Election Security Measures – The Gap
  - Computerized Voting Systems –Security Vulnerabilities
  - Cyber Security – Potential Attack Surfaces
- Cybersecurity Functions Framework (HB 472/SB274)
  - Ohio Voting System Certification – The Solution
  - Expands Ohio Cyber Reserve (OHCyR)
  - Defined Roles & Responsibilities
  - Cybersecurity Assessment Reviewers – Qualification
  - Enhanced Vendor Risk Assessments
  - Vendor Cyber Certifiability – Requirement Standards
  - Security Assessor Reviewer Restrictions
- Election System Security Review:10-Step Assessment Process
  - Security Controls – Compliance Standards & Certifications
  - ISO/IEC 20243 – Open Trusted Technology Provider Standard (OTTPs)
  - Summary Recap

Assessing Security Risk to Election Infrastructure

Private Vendors play a central role in American elections ~ Prime Target

U.S. Senate Intelligence Committee Report (2018)

Publications | Intelligence Committee (senate.gov) –
Russian Targeting of Election Infrastructure



Home > Publications > Publications

Publications

Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations

May 6, 2018

Overview

In 2016, cyber actors affiliated with the Russian Government conducted an unprecedented, coordinated cyber campaign against state election infrastructure. Russian actors scanned databases for vulnerabilities, attempted intrusions, and in a small number of cases successfully penetrated a voter registration database. This activity was part of a larger campaign to prepare to undermine confidence in the voting process. The Committee has not seen any evidence that vote tallies were manipulated or that voter registration information was deleted or modified.

- The Committee has limited information about whether, and to what extent, state and local officials carried out forensic or other examination of election infrastructure systems in order to confirm whether election-related systems were compromised. It is possible that additional activity occurred and has not yet been uncovered.

Key Takeaway:

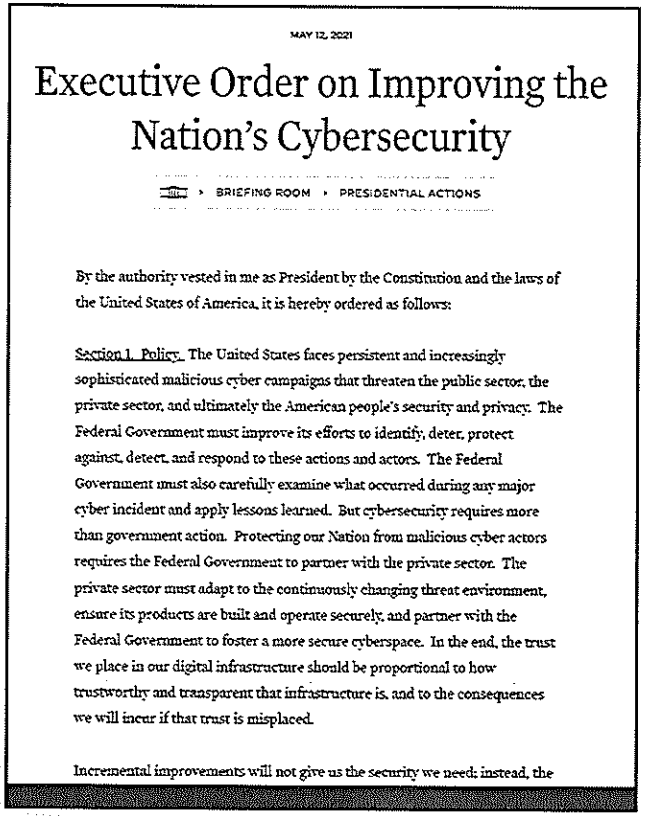
"State local, territorial, tribal, and federal government authorities have very little insight into the cyber security practices of [election] vendors"

Impossible to assess risk to vendors or impact to election security Without risk management framework

Executive Order 14028 – Improving the Nation's Cybersecurity (2021)

Key Highlights: Enhanced Vendor Risk Assessments

- **Growing emphasis on software security in supply chains**
- **Creates *higher standards for software verification techniques*** and other software ***supply chain controls***
- **Perform additional scrutiny on vendor Software Development Lifecycle (SDLC) capabilities,** security posture, and risks associated with Foreign Ownership, Control, or Influence (FOCI)



MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM › PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

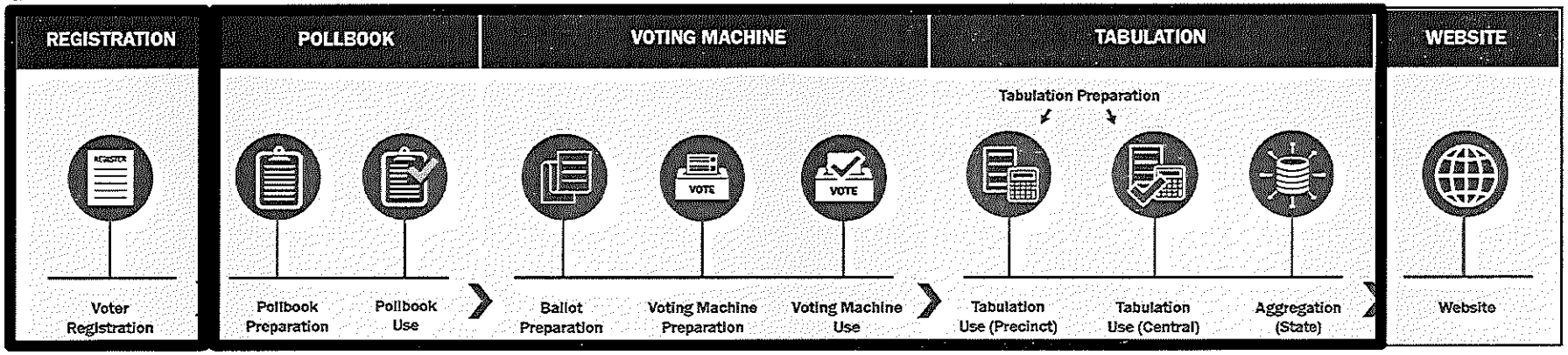
Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the

Federal government placing additional scrutiny on the software that vendors produce

Election "Critical" Infrastructure Overview

S.B. 14 Current scope of OH ***Board of Voting Machine Examiners*** equipment approval



Who has oversight of election vendors and authority to certify?

Where's the Critical Gap?

LIMITED TRANSPARENCY & ACCOUNTABILITY INTO VENDOR-DEVELOPER SECURITY PRACTICES

Ohio has opportunity to empower a State level Cyber security review team to conduct system security design and vulnerability verification

Vendor - Products and Services Overview

Vendors Present Points of Attack into Election Infrastructure

Registration Database - No Federal or State certification standard

Voter registration info is housed in statewide databases that in many jurisdictions are created or maintained by a vendor.

Ballot Programming - No Federal or State certification standard

Prior to every election, voting machines must be programmed with a memory card or USB stick to display the ballot or read and count votes. Vendors provide the software.

Electronic Pollbooks – No Federal or State certification standard

On Election Day, poll workers in jurisdictions check in voters using electronic pollbooks, usually provided by a vendor.

Voting Systems – Only partial voluntary certification standards at federal level

Jurisdictions use a variety of voting machines, all provided by vendors.

Election Night Reporting - No Federal or State certification standard

On election night, the general public can view election results through reporting websites provided by vendors.

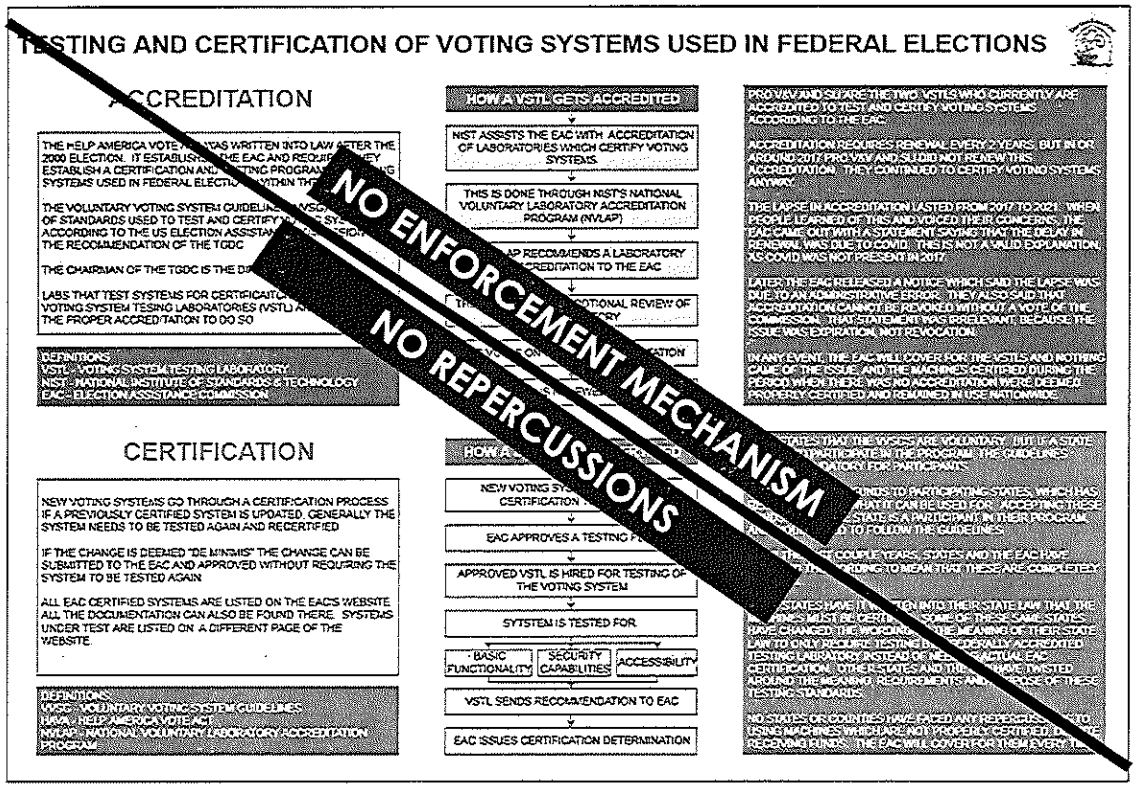
Postelection Audits - No Federal or State certification standard

After an election, vendors and their equipment play a role in checking that the equipment and procedures used to count votes worked properly and that the election yielded the correct results.

Ohio law for voting machine certification based on federal voluntary guidelines

Federal Testing & Certification Process – The Problem

Federal Election Assistance Commission (EAC)



Questionable Vendor Affiliation Influence

Only 2 National Voting System Labs

- Pro V&V & SLI
- Tests biased by manufacturer design, influence and funding

Test Objectivity & Oversight Deficit

- EAC lab accreditation delinquent 2017-2021
  - ***Voting systems still being certified to 2005 security standards (VVSG 1.0)***
  - Problems in multiple states (VA, NC, AZ)
  - No independent vendor cybersecurity attestation as criteria for certification

EAC does not have statutory authority to certify most election vendors

Ohio Law Disconnect with Federal Law

Current approved voting system certification standard is VVSG 2.0 (2021)

	Certified Votings Systems	Election Assistance Commission Test & Certification Program		
	Voting System (Name/Version)	Manufacturer	Testing Standard	Date Certified
	Assure 1.2	Premier Election Solutions, Inc. (formerly Diebold Election Systems, Inc.)	VSS 2002	8/6/2009
4	ClearVote 2.0	Clear Ballot Group, Inc.	VVSG 1.0 (2005)	10/21/2019
5	ClearVote 2.2	Clear Ballot Group, Inc.	VVSG 1.0 (2005)	12/23/2021
6	ClearVote 2.3	Clear Ballot Group, Inc.	VVSG 1.0 (2005)	10/31/2022
7	Democracy Suite 4.14 Modification	Dominion Voting Systems Corp	VVSG 1.0 (2005)	7/18/2013
8	Democracy Suite 4.14-D Modification	Dominion Voting Systems Corp	VVSG 1.0 (2005)	11/25/2014
9	Democracy Suite 4.14-E Modification	Dominion Voting Systems Corp	VVSG 1.0 (2005)	7/2/2015
10	Democracy Suite 5.0	Dominion Voting Systems Corp	VVSG 1.0 (2005)	2/8/2017
11	Democracy Suite 5.0-A	Dominion Voting Systems Corp	VVSG 1.0 (2005)	8/14/2017
12	Democracy Suite 5.17	Dominion Voting Systems Corp	VVSG 1.0 (2005)	3/16/2023
13	Democracy Suite 5.5	Dominion Voting Systems Corp	VVSG 1.0 (2005)	9/14/2018
14	Democracy Suite 5.5-A (Modification)	Dominion Voting Systems Corp	VVSG 1.0 (2005)	1/19/2019
15	Democracy Suite 5.5-C	Dominion Voting Systems Corp	VVSG 1.0 (2005)	7/9/2020
16	Democracy Suite 5.5-D	Dominion Voting Systems Corp	VVSG 1.0 (2005)	6/8/2022

WHY NOT USE 2.0?

Source: U.S. Election Assistance Commission (eac.gov)-10 Aug 23

Sec. 3506.05 "Certification of Voting & Tabulating Equipment"

(H)(4)(a) "Any voting machine, marking device, or automatic tabulating equipment used in this state shall meet, ***as a condition of continued certification and use, the voting system standards adopted by the federal election commission in 2002 OR*** *voluntary voting system guidelines most recently adopted by the election assistance commission."*

OH Law Disconnect

National Association of State Election Directors:
"Voting systems certified to the [old standard] will remain federally certified after November 15th 2023, and jurisdictions can continue using & purchasing those systems consistent with state laws and regulations." –Mar 2023

Transfer of voting system standards authority from FEC to the EAC under 2002 HAVA, supersedes Ohio's 2016 law citing FEC as system certification entity

Current Law vs. Standard (Election Systems)

1 Ohio Law (2006) ⟷ Ohio SoS Standard (2021) **2**

OHIO LAWS & ADMINISTRATIVE RULES
LEGISLATIVE SERVICE COMMISSION

HOME LAWS ABOUT CONTACT RELATED SITES GO TO

The Legislative Service Commission staff updates the Revised Code on an ongoing basis, as it completes its act review of during some times of the year, depending on the volume of enacted legislation.

Section 3506.23 | Voting machines not to be connected to internet.
Ohio Revised Code Title 35 Elections Chapter 3506 Voting And Tabulating Equipment

Previous Next

Effective: May 2, 2006 *Latest Legislation: House Bill 5 - 126th General Assembly* *PDF: Download Authenticated PDF*

A voting machine shall not be connected to the internet.

Ohio's current laws leave voting systems unprotected from cyber attacks

Ohio Voting System Requirements Matrix
Revised June 15, 2021

3. **Equipment has been certified by an independent testing authority as meeting or exceeding the minimum requirements of the U.S. Election Assistance Commission voting system standards (OAC 111:3-9-08(C)(15)).**

Acceptable ☐ Not Acceptable ☐

Covered in EAC Test Report/VSTL Test Materials? Yes ☐ No ☐ N/A ☐
Additional Information Concerning Testing Information:

Comments:

4. **A voting machine shall not be connected to the Internet (R.C. 3506.23). A voting system or voting machine is prohibited from containing any wireless communication hardware or software components.**

Acceptable ☐ Not Acceptable ☐

Covered in EAC Test Report/VSTL Test Materials? Yes ☐ No ☐ N/A ☐
Additional Information Concerning Testing Information:

Comments:

Update Ohio law with Wireless Communication Restrictions:
"Voting systems must not be capable of establishing wireless connections"

4

Make Current SoS Rule OH Law:
"A voting system or voting machine is prohibited from containing any wireless communication hardware or software components"

3

5

As condition of certification, enforce security development practices & previous build activities disclosure requirements upon election system vendor-developers

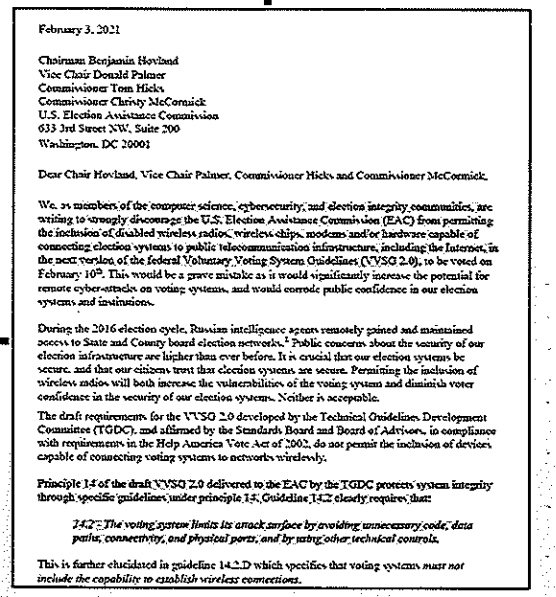
Voting System Certification Issues & Challenges

Computerized Voting System Security Vulnerabilities

EAC VVSG 2.0 standards will NOT mitigate ***known remote access threat***

25 leading computer science, cybersecurity & election integrity communities experts objected **to EAC inclusion of *disabled wireless radio, wireless chips, modems and/or hardware*** *capable* of connecting election systems to public telecom infrastructure in ***Voluntary Voting System Guidelines (VVSG 2.0)***

VVSG 2.0 Approval objection letter to Election Assistance Commission



February 3, 2021

Chairman Benjamin Hovland
Vice Chair Donald Palmer
Commissioner Tom Hicks
Commissioner Christy McCormick
U.S. Election Assistance Commission
633 3rd Street NW, Suite 200
Washington, DC 20001

Dear Chair Hovland, Vice Chair Palmer, Commissioner Hicks and Commissioner McCormick,

We, as members of the computer science, cybersecurity, and election integrity communities, are writing to strongly discourage the U.S. Election Assistance Commission (EAC) from permitting the inclusion of disabled wireless radios, wireless chips, modems and/or hardware capable of connecting election systems to public telecommunication infrastructure, including the Internet, in the next version of the federal Voluntary Voting System Guidelines (VVSG 2.0), to be voted on February 10th. This would be a grave mistake as it would significantly increase the potential for remote cyber-attacks on voting systems, and would corrode public confidence in our election systems and institutions.

During the 2016 election cycle, Russian intelligence agents remotely gained and maintained access to State and County board election networks.[1] Public concerns about the security of our election infrastructure are higher than ever before. It is crucial that our election systems be secure, and that our citizens trust that election systems are secure. Permitting the inclusion of wireless radios will both increase the vulnerabilities of the voting system and diminish voter confidence in the security of our election systems. Neither is acceptable.

The draft requirements for the VVSG 2.0 developed by the Technical Guidelines Development Committee (TGDC), and affirmed by the Standards Board and Board of Advisors, in compliance with requirements in the Help America Vote Act of 2002, do not permit the inclusion of devices capable of connecting voting systems to networks wirelessly.

Principle 14 of the draft VVSG 2.0 delivered to the EAC by the TGDC protects system integrity through specific guidelines; under principle 14, Guideline 14.2 clearly requires that:

> *14.2 The voting system limits its attack surface by avoiding unnecessary code, data paths, connectivity, and physical ports, and by using other technical controls.*

This is further elucidated in guideline 14.2.D which specifies that voting systems *must not include the capability to establish wireless connections.*

EAC removed recommended prohibitions for wireless networking configuration

- **Permits networking capability** ⟷ ***"Grave mistake as it would significantly increase the potential for remote cyber-attacks on voting systems"***
- **Known remote system access methods-**
  - **Unintentional misconfiguration**
  - **A software update**
  - **Technical error**

Ohio law should require voting system equipment certification standards with greater rigor than EAC published VVSG 2.0

Current Ohio Election Security Measures – The Gap

Albert
CIS Network Monitoring

- In 2019, OH initiated a ***network security monitoring service*** w/DHS Center for Internet Security

  Special intrusion detection devices known as ***"Albert Sensors"*** installed across 88 counties

  ** **Intent to identify malicious or potentially harmful network activity** ***"based on known signatures"***

  The Gap: Inability to detect poor practices and weak system design due to lack of visibility into vendors development security practices

  The Approach: Evaluate ***system security design upfront to discover system threats, vulnerabilities, malware and malicious software*** during *system production and build prior to customer delivery*

  No vendor directed by State to comply with security build practices as condition of certification

Full cybersecurity unattainable without vendor security development practices disclosure

Computerized Voting Systems - Security Vulnerabilities

- ***Dominion ImageCast X (ICX) Ballot Marking Device (BMD)***
  - *Principal Findings* – **"ICX suffers from critical vulnerabilities" Altered both QR codes and human text**

Most Serious Vulnerabilities– (Halderman Report 2023)

- Attackers ***altered QR codes on printed ballots*** to modify voters' selections
- ***Software updates*** lead to potential access/***malware install in polling place***
- ***Forged & manipulated smart cards*** used unlock any ICX and install malware
- ***Altered election definition*** **files** via arbitrary code, ***can exploit all machines in the county***
- ***Access to scanner's memory card violate ballot secrecy*** by dishonest election worker
- Alteration of audit logs through access of ***unnecessary Android applications***
- ***Obtained county-wide keys via access to single ICX and Poll Worker Card & Pin,***
  - *All scanners & BMDs share same set of cryptographic keys for authentication*

Key Takeaway: ***BMDs and DREs in use in Ohio "developed without sufficient attention to security using standard software engineering practices. A small mistake can lead to complete exploitation."***

BMDs and DREs are "not sufficiently secured to withstand vote-altering attacks"

Cyber Security – Potential Attack Surfaces

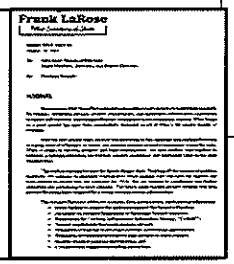
Application-Level Threats
- Input Validation Attacks
- Authentication and Authorization
- Data Exposure
- Business Logic Flaws

Software Development Life Cycle (SDLC) Threats
- Requirement Phase
- Design Phase
- Implementation Phase
- Testing Phase
- Deployment Phase
- Maintenance Phase

FEDERAL SECURITY PARTNERSHIP [DHS/OH SoS)

UPDATE STATE SECURITY LEGISLATION

Network Level Threats
- Perimeter Security
- Data Transmission
- ***Endpoint Security***
- Internal Threats



SoS Directive 2023-16 (Aug 28th 2023)

Frank LaRose
Ohio Secretary of State

Contractual Aspects Implications
- Security Requirements
- Compliance and Standards
- Liabilities and Indemnities
- Data Ownership and Privacy

Evaluate *network security at the access, application and data levels* for more secure, compliant and resiient operational environment

Cybersecurity Functions Framework

MISSING

Status of Voting System
- *In-Development*

Core Functions
- *Identify*
- *Protect*

Security review of vendor practices

1 *State Level Partnership (Certification)*

Collaboration

Ohio Cyber Reserve
+
Board of Voting Machine Examiners

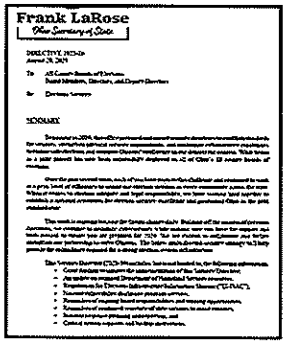
CURRENT

Status of Voting System
- Delivered
- Fielded

Core Functions
- Detect
- Respond
- Recovery

2 Federal Level Partnership

End point security services (ESS)


Frank LaRose
Ohio Secretary of State

DIRECTIVE 2023-16
August 28, 2023

To: All County Boards of Elections, Board Members, Directors, and Deputy Directors

From: Secretary LaRose

SUMMARY

SoS Directive 2023-16 (Aug 28th 2023)

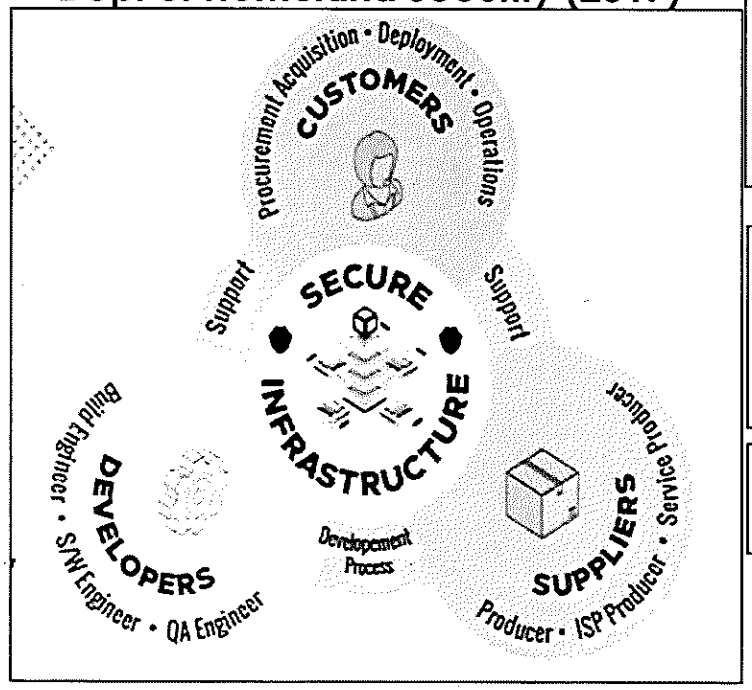
Collaboration

Ohio SoS
+
Dept of Homeland Security/
Center for Internet Security
*Crowdstrike (Vendor)

Ohio solves for *Detection, Responding & Recovering* but NOT *Identifying, Protecting*
The earlier security flaws are identified in development & remediated, the less effort and cost

Ohio Voting System Certification – The Solution

Elections are
"National Critical Infrastructure"
-Dept of Homeland Security (2017)

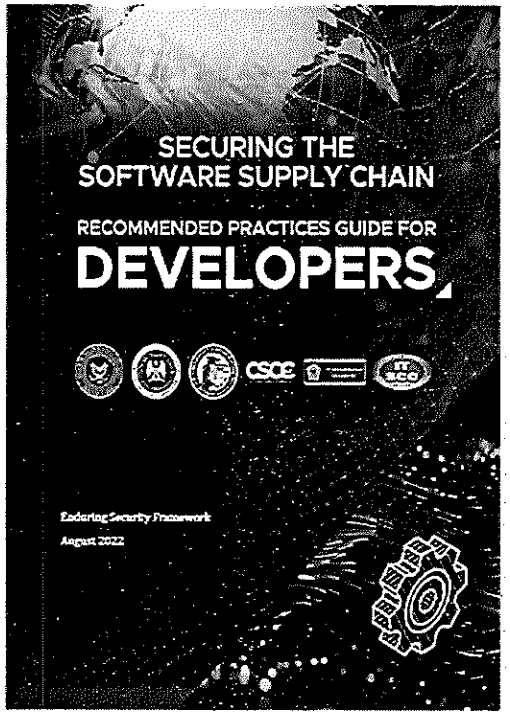


Codify following provisions into law:

1. ***Codify SoS system requirement rule*** prohibiting wireless hardware/software component in voting machines

2. ***Vendors adhere to federal security development practices*** *and disclose voting system development practices* ***as condition of certification***

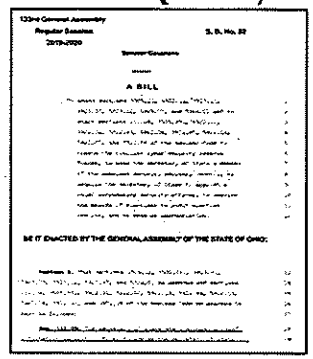
3. ***Introduce in-state 3rd party Cyber Security Reviews***



Empower OHIO CYBER RESERVE to lead certification security reviews in partnership with SOS as a pre-requisite to election voting system selection and County BOE procurement

H.B. 472/S.B. 274 Expands Ohio Cyber Reserve (OHCyR)

S.B. 52 (2019)

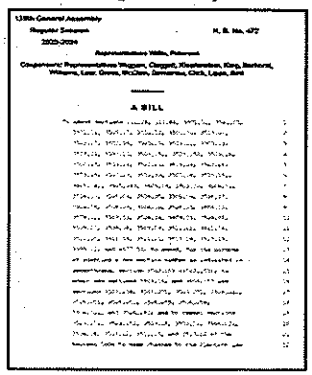


Mission: OHCyR 1.0

- Assist governmental entities with Cybersecurity vulnerabilities & provide recommendations to reduce cyber threats

OHCyR established under Adjutant General 2019 (S.B. 52)

HB 472/SB 274 (2024)



Proposed Roles/Responsibilities: OHCyR 2.0

- Authorized Security Reviewer/Supervisory Control
  - Coord w/Voting System Vendors/3PAOs/OH SoS Board of Voting System Examiners
  - Contract w/3rd Party Security Assessor (3PAO)
  - Oversee 3PAO system security verification review
  - Review/Submit system ***vulnerability disclosure report*** to SoS

OHCyR available to oversee or perform security review assessments and vulnerability testing and reporting of election voting systems

HB 472/SB 274 Legislation– Defined Roles & Responsibilities

- **Secretary of State (SoS) Shall:**
  - Devise requirements for the recommendation, certification, and continued certification of the voting systems to be used
  - Publicly report all contracts, service agreements, business proposals, payment invoices, & grants between SoS and the boards of elections with voting system vendor and registered non-governmental organizations subject to disclosure
  - Maintain public web site identifying & providing access to all existing voting system & NSGO existing contracts, service agreements, proposals, payment invoices, and grants related to election services and support activities
- **SoS Board of Voting Systems Examiners Shall:**
  - Include summary findings of 3rd Party security review including:
    - Identified security vulnerability findings
    - Written statement by the voting system vendor on qualified actions to remediate known security vulnerabilities
- **Voting System Vendors Shall:**
  - Submit their system to an examination or test as condition of certification
  - Notify SoS of any security vulnerabilities & corrective actions to change hardware or software that alters the methods of recording voter intent, system security, voter privacy, retention of the vote, communication of records or connection between the system or other systems
- **3rd Party Security Assessment Reviewer Shall:**
  - Shall periodically examine, test, and inspect certified voting systems to determine compliance

Reduce election system risk by requiring vendor-developers disclose system development security practices, foreign ownership and attest to software supply chain integrity

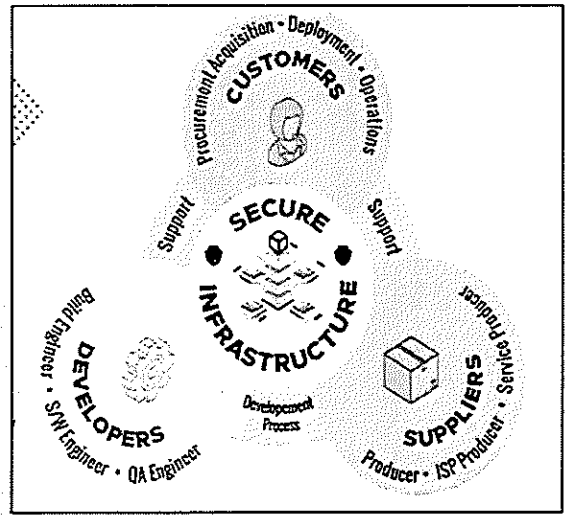
Cybersecurity Assessment Reviewers - Qualifications

- Person shall be a ***U.S. Citizen, no criminal record, no influence or control of entities outside U.S.***
- Minimum of ***5-years management or analyst experience in information security***
- ***Pass information security exam*** in the following areas:
  - Information technology risk management, identification, mitigation, and compliance
  - Information security incident management
  - Information security program development and management
  - Risk and control monitoring and reporting
  - Access control systems and methodology
  - Business continuity planning and disaster recovery planning
  - Physical security of computer systems
  - Networking security
  - Security architecture application and systems development
- Person or person's employer or business ***shall not receive any form of compensation from, or have any affiliation with, the voting system vendor***

SoS Board of Voting Machine Examiners (BVME) are not Cybersecurity credentialed
Current review limited to vendor attestation (weak) checklist

HB 472/SB 274 - Enhanced Vendor Risk Assessments

- <u>Voting System Vendors & Developers shall:</u>
  - Permit 3rd party assessment reviews
  - Disclose open-source components in operating systems, development frameworks & data utilization
  - Periodically attest to adherence of NIST most recent secure software development framework (SSDF) derived in SP 800-218
  - Extend foundational capability to subsidiary suppliers designated w/in outside-in analysis or software bill of materials (SBOM)
  - Include flow-down requirements to subsidiary suppliers in agreements for secure development, delivery, operational support & maintenance of software
  - Use suppliers who provide a software security label or data sheet that includes info on the background, qualifications, skills, and citizenship of key personnel involved in building software for all products
- Periodically submit and upon 3rd party request applicable SSDF requirements:
  - Automated build deployments
  - Pre-Production Testing
  - Automatic Rollbacks
  - Staggered production deployments
  - Low Level artifacts



Secure Software Development Framework (SSDF): NIST SP 800-218 Recommendations for Mitigating the Risk of Software Vulnerabilities

Vendor Cyber Certifiability – Requirement Standards

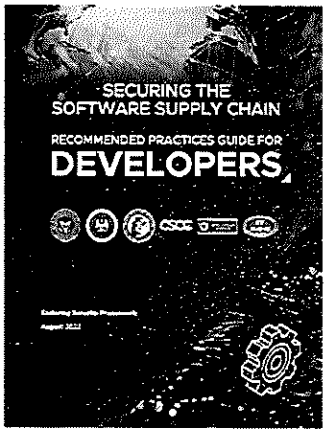
Appendix D: Artifacts and Checklists

Producible Items

1. High-level Secure Development Lifecycle Process Document
2. Product Readiness Checklist
3. Product Support/Response Plan
4. Software Bill of Material (SBOM)
5. Architecture/Design Documents
6. Developer Training Certificates/Training Completion Statistics/data
7. Threat Model Results Document
8. High-level Software Security Test Plan and Results
9. Automatic and Manual Dynamic and Static Security/Vulnerability Reports (Security Scanning Results) Reports
10. Open Source Review Process Document and Allowed List
11. Build Log
12. Secure Development Build Configurations Listing
13. Third-Party Software Tool-Chains List

1

2



OHIO CYBER RESERVE
OhCR

Decision Point

Frank LaRose
Ohio Secretary of State

4

3

OH BOARD of VOTING SYSTEMS EXAMINERS

Ohio Cyber Reserve will perform cyber security verification of vendor-developer systems and submit report to OH SoS for Certification determination and public disclosure disclosure

Security Assessor Reviewer Restrictions

- **Prohibitions:**
  - No voting system shall be used in this state if any of the following persons have pecuniary interest in, or affiliation with, the voting system vendor
    - SoS or any election official in the office of the SoS
    - Any member of the board of voting systems examiners
    - Any person who conducts a cybersecurity assessment of the voting system
    - Any relative of a person listed (i.e. person's spouse, parent, stepparent, parent-in-law, grandparent, etc...)

Current voting system presents conflict of interest, election officials appointed to the SoS Board of Voting Machine Examiners are both users and authorizers of the voting systems

Election System Security Review:10-Step Assessment Process

1. Receive authority and direction from State to conduct assessment and accreditation of State election system components (H.B. 472/S.B. 274)

2. Select external auditor with credentialing in ISO/IEC 20243 assessments to conduct the assessment (OHCyR)

3. Develop a gap analysis checklist tailored to State election systems (OHCyR)

4. Develop an SCRM assessment plan providing the scope, equipment list, location, secure storage, chain of custody, credentialed assessor list, tailored checklist, and start/end dates based on the quantity of assessors and equipment. (OHCyR)

5. Develop a procedure for handling assessment exceptions and findings. (OHCyR)

6. Develop minimum criteria for assessment acceptance and accreditation based on any exceptions. (H.B 472/S.B 274/OHCyR)

7. Conduct the assessment and provide a vulnerability report with findings for all controls. (3rd Party Security Assessment Reviewer)

8. Provide an authorization letter from the State Authorizing official to authorize the systems for elections (SoS/Board of System Examiners)

9. Develop a contingency plan for failure to authorize (such as hand counting of paper ballots). (County Board of Elections)

10. Set up a program to monitor and control the election system chain of custody during elections (SoS/County Board of Elections)

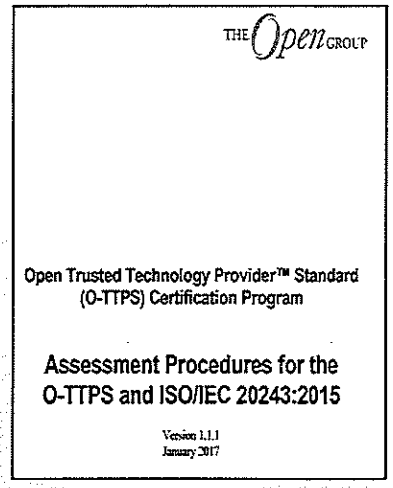
Proposed 10-Step Assessment and Review Process for OH Voting Systems Certification

Security Controls – Compliance Standards & Certifications

- Apply to an any component of an information system that stores, processes or transmits information
- State election systems required to follow risk management requirements of Federal Critical Infrastructure Protection (CIP)

  - Federal Information Security Modernization Act
  - FIPS 200
  - ISO/IEC 20243
  - NIST SP800 series
    - NIST SP 800-218
    - NIST SP 800-53a

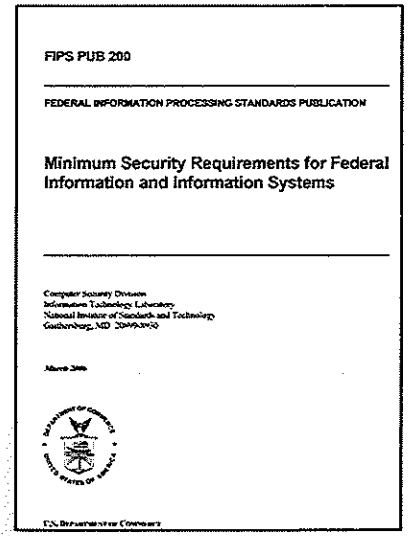
FY 2024
Inspector General
Federal Information
Security Modernization Act of 2014
(FISMA) Metrics
Evaluator's Guide


THE Open GROUP

Open Trusted Technology Provider™ Standard (O-TTPS) Certification Program

Assessment Procedures for the O-TTPS and ISO/IEC 20243:2015

Version 1.1.1
January 2017


FIPS PUB 200

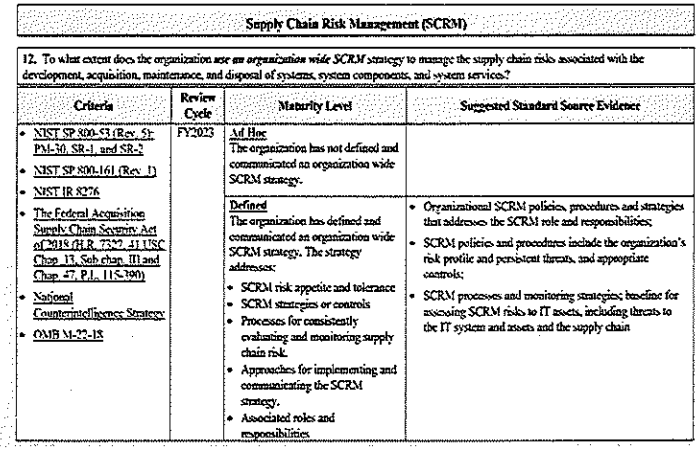
FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Minimum Security Requirements for Federal Information and Information Systems

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

March 2006

U.S. Department of Commerce



Supply Chain Risk Management (SCRM)

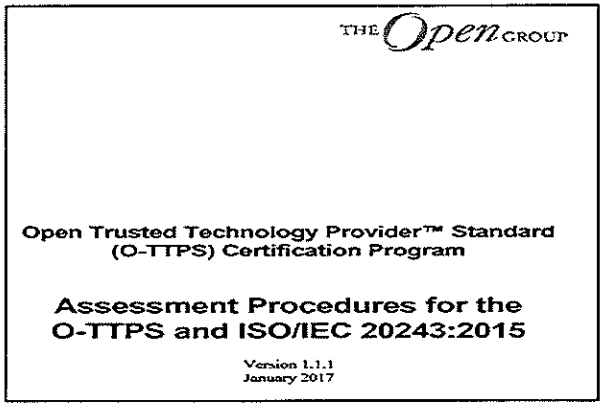
12. To what extent does the organization *use an organization wide SCRM* strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53 (Rev. 5): PM-30, SR-1, and SR-2 • NIST SP 800-161 (Rev. 1) • NIST IR 8276 • The Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13, Sub chap. III and Chap. 47, P.L. 115-390) • National Counterintelligence Strategy • OMB M-22-18	FY2023	Ad Hoc The organization has not defined and communicated an organization wide SCRM strategy.	
		Defined The organization has defined and communicated an organization wide SCRM strategy. The strategy addresses: • SCRM risk appetite and tolerance • SCRM strategies or controls • Processes for consistently evaluating and monitoring supply chain risk. • Approaches for implementing and communicating the SCRM strategy. • Associated roles and responsibilities	• Organizational SCRM policies, procedures and strategies that addresses the SCRM role and responsibilities; • SCRM policies and procedures include the organization's risk profile and persistent threats, and appropriate controls; • SCRM processes and monitoring strategies; baseline for assessing SCRM risks to IT assets, including threats to the IT system and assets and the supply chain

State Election Systems are NOT compliant with risk management requirements of Federal Critical Infrastructure Protection (CIP)

ISO/IEC 20243 – Open Trusted Technology Provider Standard (OTTPs)

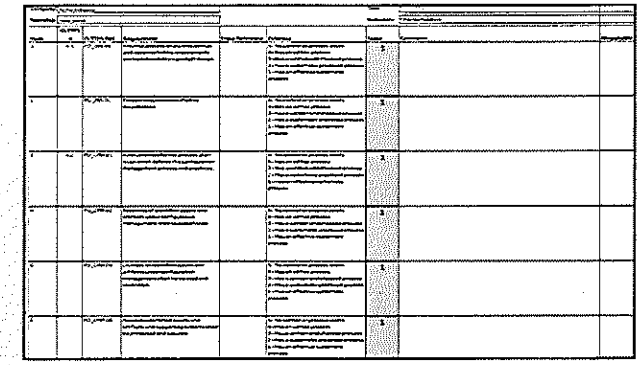
- ***Global standard*** for technology providers, integrators, original equipment manufacturers (OEMs), and hardware/software providers ***(i.e. voting system vendors)***
- Aims to ***mitigate risk*** of counterfeit and maliciously tainted products w/supply chains, requires proof of system incorruptibility
- Focuses on ***best practices for secure development, manufacturing, and supply chain processes***
- Organized into categories:
  - Product development/engineering
  - Secure development/engineering,
  - Supply chain security
  - Product evaluation


THE Open GROUP

Open Trusted Technology Provider™ Standard (O-TTPS) Certification Program

Assessment Procedures for the O-TTPS and ISO/IEC 20243:2015

Version 1.1.1
January 2017



Gap Analysis Checklist
(55 Controls to verify hardware & software design of system)

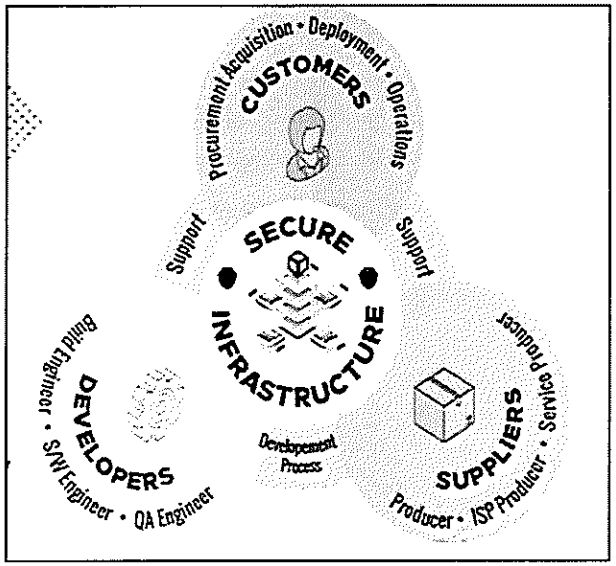
OHCyR has capability and capacity to certify organizations and oversee 3rd Party Security Assessors conducting validation and vulnerability analysis of voting systems

Summary

Challenges

- ***No federal certification standards for most voting systems*** products and services
- Election systems ***continue to certify to obsolete 2005 security standards*** through 2023
- ***No election vendor oversight*** for software supply chain integrity & security development practices
- ***BMD and DRE voting machines not secured to withstand "vote altering attacks,"*** known threats can **falsify** voter intent & fail ***auditability under HAVA Title III via QR code***

Recap



Questions?

Solutions

- ***Codify SoS system requirement rule prohibiting wireless hardware/software components*** in voting machines
- **Vendors shall adhere to federal security development practices**, disclose software byproducts (i.e. artifacts) & agree to 3rd party security review **as condition of certification**
- **Direct Ohio Cyber Reserve to conduct security analysis review** of election vendor systems
- **Specify County machine opt-clause for system de-certification** & hand-marked paper ballot counting pilot studies

BACKUP

12 Most Common Types of Cyberattacks

1. Malware – Program or crode created with intent to harm a computer, network or server
2. Denial-of-Service (DoS) Attacks – Floods a network with false attacks
3. Phishing - Attack that uses email, phone, social media to entice victim to share sensitive information
4. Spoofing - Attacker disguises themselves as a trusted source
5. Identity-Based Attacks – User's credentials compromised and attacker impersonates user
6. Code Injection Attacks – Attacker injects malicious code into a vulnerable computer or network to change its course of action
7. Supply Chain Attacks – Targets a trusted-3rd party vendor who offers services or software vital to the supply chain
8. Social Engineering Attacks – Attackers use psychological tactics to manipulate people into taking desired action
9. Insider Threats – Internal actors that pose a threat to an organization
10. DNS Tunneling – Type of attacj that leverages domain name system (DNS) queries ad responses to bypass security measures
11. IoT-Based Attacks – Attack that targets an Internet-of-Things device or network to assume control or steal data
12. AI-Powered Attacks – Leverage tools to get access to a network or steal sensitive information

Election Infrastructure – Cost Benefit Analysis

Butler County, Ohio ~ 1x Purchase Agreement $6.1M

- $6.1M X 88 Counties = ~ +$536M for Ohio Vendor Contracts

EXHIBIT A

TO THE VOTING SYSTEM AND SERVICES AGREEMENT
BY AND BETWEEN DOMINION VOTING SYSTEMS, INC.
AND THE COUNTY OF BUTLER, OHIO

PRICING SUMMARY AND DELIVERABLES DESCRIPTION

1. Pricing Summary - Prices of equipment, technical facilities, software, and other related services for voting, vote counting, and result processing. All pricing in U.S. Dollars.

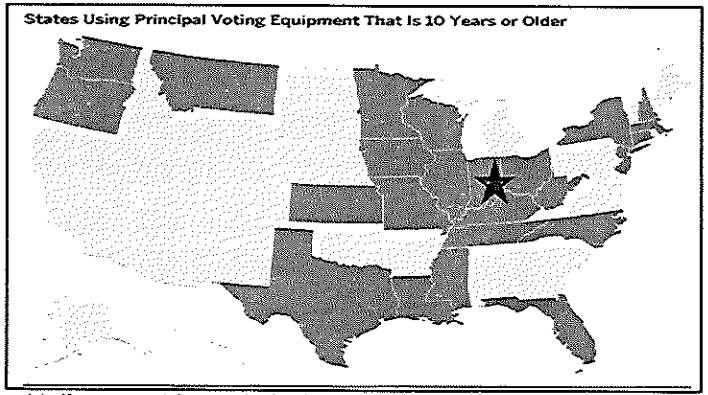
Table A: State-Funded Items pursuant to Exhibit C

DESCRIPTION	QTY	UNIT PRICE	EXTENSION PRICE
Central Scanning Solution: Absentee / Vote By Mail Hardware			
ImageCast Central Kit: Canon DR-G1130 high speed document scanner includes: ImageCast Central Software, Dell OptiPlex All-In-One, iButton programmer and key, cables	3	$ 25,000.00	$ 75,000.00
Sub-Total:			$75,000.00
In-Person Voting Solution: Polling Location Hardware			
ImageCast X DRE w/VVPAT (21 inch) Kit includes: ICX Firmware, Tablet, 5 voter activation cards, VVPAT, cables, power cord	1,500	$ 3,500.00	$5,250,000.00
ATI Accessible Voting Kit for ICX USB	100	$ 375.00	$37,500.00
ImageCast X Voting Leg Stand	1,500	$250.00	$375,000.00
M&P System includes Oki Data C931E printer, laptop, cables	3	$11,560.00	$34,680.00
ICX Pollworker Smartcard	900	$ 8.00	$7,200.00
ICX Technician Smartcard	150	$ 8.00	$1,200.00
Dual Bay Battery Charger	50	$ 165.00	$8,250.00
8GB USB Flash Drive	1,500	$17.00	$25,500.00
Sub-Total:			$5,739,330.00
Election Management Hardware			
Democracy Suite EMS Express Server - up to 7 clients	1	$ 17,000.00	$ 17,000.00
EMS Client Workstation Configuration Kit	1	$ 2,500.00	$ 2,500.00
EMS Report Printer	2	$ 250.00	$ 500.00
Adjudication workstation	2	$1,900.00	$3,800.00
Smart Card Reader/Writer	5	$22.00	$110.00
Sub-Total:			$23,910.00
Software License Fee			
Democracy Suite (EMS) Application	1	$ 170,000.00	$ 170,000.00
Adjudication Software	1	$35,000.00	$35,000.00
Mobile Ballot Printing	1	$6,500.00	$6,500.00
			$211,500.00
Implementation Services	Days		
Voting System Deployment (e.g., software, installation & configuration, acceptance testing, etc.)	70	$ 2,000.00	$140,000.00

Dominion Voting Systems Inc.
Exhibit A – 5.15.2019

Butler County Purchase Agreement
Page 1 of 7

What is the <u>cost-benefit analysis</u> of an exclusively electronic voting system vs. blend of hand-marked paper ballot counting?



<u>Voting Machines at Risk in 2022 | Brennan Center for Justice</u>

Knowing computerized voting systems have known technical design security flaws and remote system threat access points enabled by activated wireless configuration that enable cyber exploitation and attack vulnerabilities....

How do we secure tens of millions of dollars worth of computerized voting system investment and restore public confidence without introducing real vendor accountability or oversight transparency of product development?

Reduce election system risk by requiring vendor-developers disclose system development security practices, foreign ownership and attest to software supply chain integrity

Zero Trust Cybersecurity

What is Zero Trust?

- Zero Trust is a cybersecurity philosophy based on the premise that threats can arise internally and externally. With Zero Trust, no user, system, or service should automatically be trusted, regardless of its location within or outside the network. Providing an added layer of security to protect sensitive data and applications, Zero Trust only grants access to authenticated and authorised users and devices. And in the event of a data breach, compartmentalising access to individual resources limits potential damage.

Greene County - Opposing Resolution on DREs

Objectivity Deficit – Conflict of interest

- "Voting Machine contractor employees are involved in the audit and certification of their own machines before, during and after the election process"

Non-transparency – Questionable integrity of election process

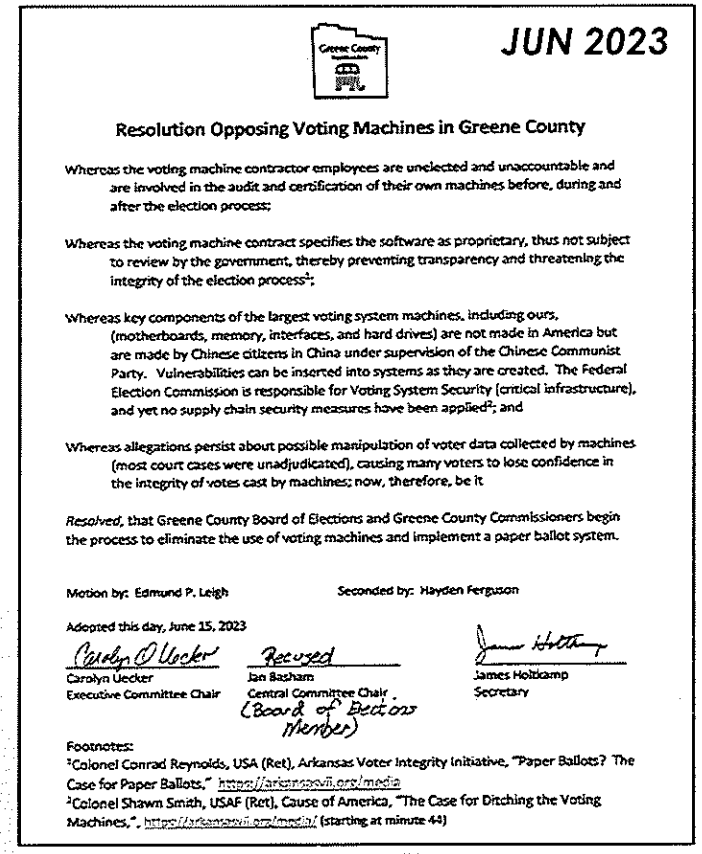
- "Voting machine contract specifies the software as proprietary, not subject to review by the government"

Supply chain integrity – Unaccounted and non-reviewable

- "Key components of voting system machines, (motherboards, memory, interfaces, and hard drives) are not made in America but made by Chinese citizens"
- "EAC is responsible for Voting system security and yet no supply chain security measures have been applied."

Public confidence in computerized voting systems decreasing

- "Allegations persist about possible manipulation of voter data (most court cases were unadjudicated), causing voters to lose confidence in integrity of votes cast by machines"



JUN 2023

Resolution Opposing Voting Machines in Greene County

Whereas the voting machine contractor employees are unelected and unaccountable and are involved in the audit and certification of their own machines before, during and after the election process;

Whereas the voting machine contract specifies the software as proprietary, thus not subject to review by the government, thereby preventing transparency and threatening the integrity of the election process[1];

Whereas key components of the largest voting system machines, including ours, (motherboards, memory, interfaces, and hard drives) are not made in America but are made by Chinese citizens in China under supervision of the Chinese Communist Party. Vulnerabilities can be inserted into systems as they are created. The Federal Election Commission is responsible for Voting System Security (critical infrastructure), and yet no supply chain security measures have been applied[2]; and

Whereas allegations persist about possible manipulation of voter data collected by machines (most court cases were unadjudicated), causing many voters to lose confidence in the integrity of votes cast by machines; now, therefore, be it

Resolved, that Greene County Board of Elections and Greene County Commissioners begin the process to eliminate the use of voting machines and implement a paper ballot system.

Motion by: Edmund P. Leigh Seconded by: Hayden Ferguson

Adopted this day, June 15, 2023

Carolyn Uecker — Executive Committee Chair
Recused — Jan Basham, Central Committee Chair (Board of Election Member)
James Holtkamp — Secretary

Footnotes:
[1]Colonel Conrad Reynolds, USA (Ret), Arkansas Voter Integrity Initiative, "Paper Ballots? The Case for Paper Ballots," https://arkansasvii.org/media
[2]Colonel Shawn Smith, USAF (Ret), Cause of America, "The Case for Ditching the Voting Machines.", https://arkansasvii.org/media/ (starting at minute 44)

All voting systems face cybersecurity risks, not all voting systems are equally vulnerable

Opt-Out Clause: Criteria & Alternatives

Establish criteria to determine primary method for casting, recording & tabulating ballots in the event a voting systems fail certification standards:

Criteria Examples:

1. "All **components** have been **designed, manufactured, integrated and assembled in the U.S.** from trusted suppliers, using trusted processes accredited by the Defense Microelectronic Activity as prescribed by Dept of Defense
2. The **source code** used in any computerized voting machine for federal elections is **made available to the public or designated state directed cyber security review entity**
3. The **ballot images and system log files from each tabulator** are recorded on a secure write-once, read-many media with clear chain of custody and **posted on the Secretary of State's website** free of charge to the public within 24-72 hours after the close of polls

- Defense Microelectronics Activity - AccreditedSuppliers.pdf (osd.mil)

What will counties do if voting systems are de-certified?

Incorporate county machine-us pt-out provision into Sec 3506.02 in event of voting system de-certification

Initiate a legislative study and/or county pilot project to study feasibility of primary hand-marked paper ballot counting at the precinct level

Revised Ohio Law - Security Certification Provisions

Vendor-Developer Provisions:

- Adopt *software supply chain integrity security development best practices**
- Require *security development build practices disclosure*
- *Include background checks and security measures for personnel**
- *Disclose vendor & subcontractor foreign ownership**
- *Requirement and processes for reporting cyber incidents**
- *Require Software Bill of Materials (SBOM)*
- Accept recurring *State-directed 3rd party regular system build audits,* penetration testing and physical site inspections
- *Accept publication of system security review team findings on SoS website* for public transparency

**Brennan Center for Justice, "A Framework for Election Vendor Oversight: Safeguarding America's Election Systems (2019)*

Update Section 3506.10 | Requirements for approval or certification of voting machines
Effective: May 7, 2004

Current Voting Machine System Certification Shortfalls

Common Misnomers: "We're secure because our voting machines are NOT connected to the internet"

- Cyber attacks and exploit compromise can derive from Machine-Hardware/Software, Operating System, Servers, Application and Data layers

Fact: Computerized voting systems have known technical design security flaws and remote system threat access points enabled by activated wireless configuration that enable cyber exploitation and attack vulnerabilities....

Fact: Currently no voting machine, marker or tabulator in the country is certified beyond 2005 security standard

All Ohio Voting Machine, Markers & Tabulators Approved for Use in 2024 are Certificated to a 2005 Federal Advisory EAC Voluntary Voting System Guideline (VVSG 1.0) Standard

Hannum, Logan

From: Eileen Watts <ewattsohio@gmail.com>
Sent: Thursday, May 16, 2024 5:06 PM
To: State Senator Theresa Gavarone; State Senator Andrew Brenner; Marcell Strbich; Gail Niederlehner; Jim Rigano; Rep91; Rep74
Subject: HB 472 Briefing for Senate bill

Hello Senator Gavarone, Senator Brenner, Representative Peterson and Representative Willis,

Ohio Election Integrity Network is inviting you to a scheduled Zoom meeting.

Topic: HB 472 briefing for Senators
Time: May 20, 2024 01:00 PM Eastern Time (US and Canada)

Join Zoom Meeting
https://zoom.us/j/95895789585?pwd=OXVlQjB0WnNuRmdNSStneDB5ZENNUT09

Meeting ID: 958 9578 9585
Passcode: 930912

One tap mobile
+13126266799,,95895789585#,,,,*930912# US (Chicago)
+16469313860,,95895789585#,,,,*930912# US

Dial by your location
- +1 312 626 6799 US (Chicago)
- +1 646 931 3860 US
- +1 929 436 2866 US (New York)
- +1 301 715 8592 US (Washington DC)
- +1 305 224 1968 US
- +1 309 205 3325 US
- +1 689 278 1000 US
- +1 719 359 4580 US
- +1 253 205 0468 US
- +1 253 215 8782 US (Tacoma)
- +1 346 248 7799 US (Houston)
- +1 360 209 5623 US
- +1 386 347 5053 US
- +1 507 473 4847 US
- +1 564 217 2000 US
- +1 669 444 9171 US
- +1 669 900 6833 US (San Jose)

Meeting ID: 958 9578 9585
Passcode: 930912

Find your local number: https://zoom.us/u/ah46AKgdL

Eileen Watts
ewattsohio@gmail.com
614-352-1010

Hannum, Logan

From: Eileen Watts <ewattsohio@gmail.com>
Sent: Thursday, May 16, 2024 5:06 PM
To: State Senator Theresa Gavarone; State Senator Andrew Brenner; Marcell Strbich; Gail Niederlehner; Jim Rigano; Rep91; Rep74
Subject: HB 472 Briefing for Senate bill

Hello Senator Gavarone, Senator Brenner, Representative Peterson and Representative Willis,

Ohio Election Integrity Network is inviting you to a scheduled Zoom meeting.

Topic: HB 472 briefing for Senators
Time: May 20, 2024 01:00 PM Eastern Time (US and Canada)

Join Zoom Meeting
https://zoom.us/j/95895789585?pwd=OXVlQjB0WnNuRmdNSStneDB5ZENNUT09

Meeting ID: 958 9578 9585
Passcode: 930912

One tap mobile
+13126266799,,95895789585#,,,,*930912# US (Chicago)
+16469313860,,95895789585#,,,,*930912# US

Dial by your location
- +1 312 626 6799 US (Chicago)
- +1 646 931 3860 US
- +1 929 436 2866 US (New York)
- +1 301 715 8592 US (Washington DC)
- +1 305 224 1968 US
- +1 309 205 3325 US
- +1 689 278 1000 US
- +1 719 359 4580 US
- +1 253 205 0468 US
- +1 253 215 8782 US (Tacoma)
- +1 346 248 7799 US (Houston)
- +1 360 209 5623 US
- +1 386 347 5053 US
- +1 507 473 4847 US
- +1 564 217 2000 US
- +1 669 444 9171 US
- +1 669 900 6833 US (San Jose)

Meeting ID: 958 9578 9585
Passcode: 930912

Find your local number: https://zoom.us/u/ah46AKgdL

Eileen Watts
ewattsohio@gmail.com
614-352-1010

Hannum, Logan

From:	mstrbic <mstrbic@protonmail.com>
Sent:	Wednesday, March 13, 2024 12:32 AM
To:	Willis, Bernard
Cc:	Gail Niederlehner; Jim Rigano
Subject:	Election Bill Follow-Up and Support Info

Bunyon,

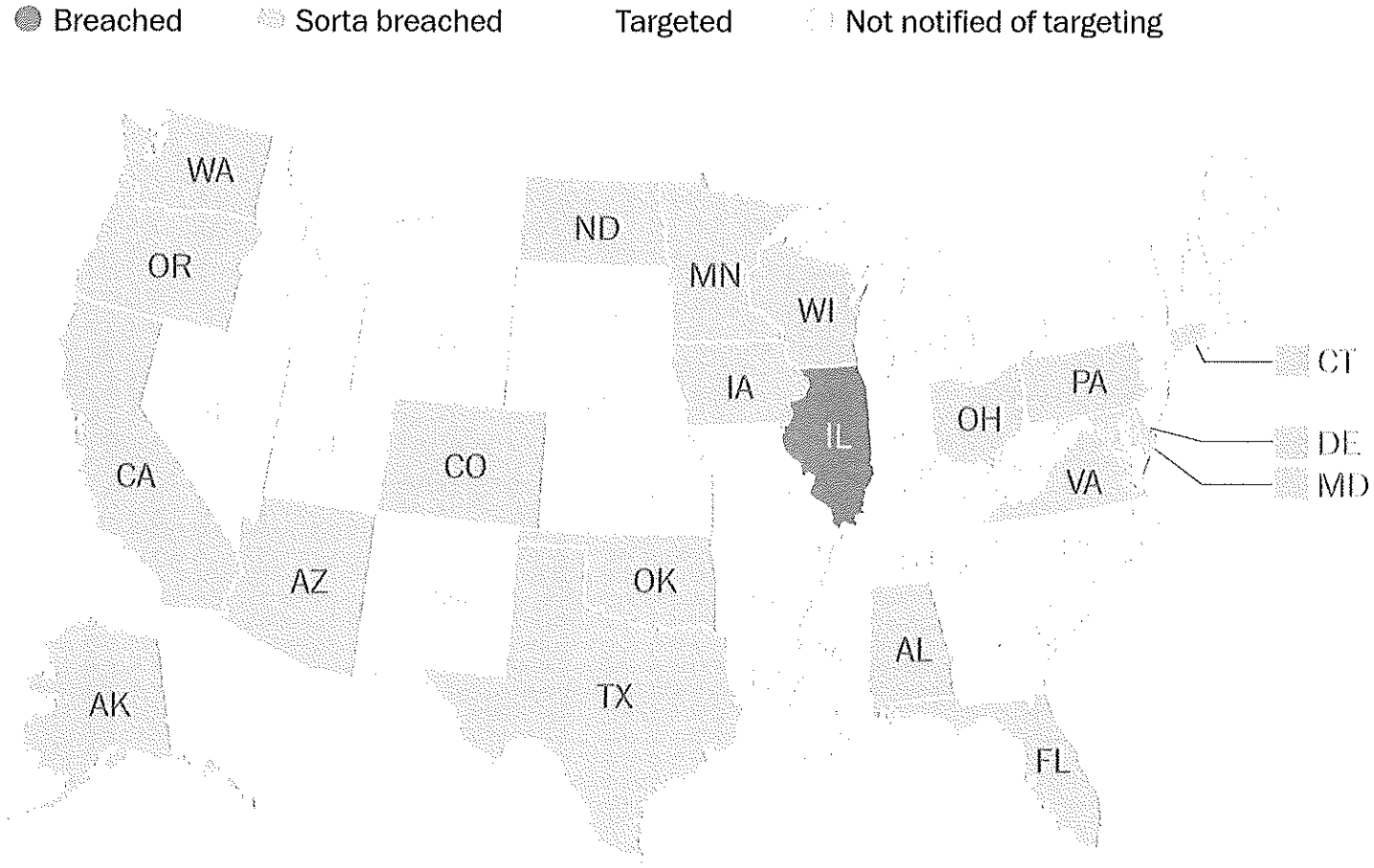
Just following up from Monday's election bill intro meeting. The Chairman specifically asked for scope and extent of Voter Registration Database breach incidents nationally. In 2019, the Senate Select Intel Committee completed a 2-year investigation and concluded seven states succumbed to Russian hacking attempts during the 2016 election cycle.

Since that report, an additional 5 States (i.e. Georgia, Alaska, Florida, Michigan, Arizona) to include the entire voter roll of the District of Columbia (2023) succumbed to database breaches. Due to the difficulty in detecting these breaches as a result of lack of anti-tamper evidence features in our current voter registration databases and aversion by law enforcement and election officials to public reporting, there are likely more instances of breaches and possible voter record alterations that are unreported.

Considering the antiquated State of our Voter Registration Databases (i.e. 2005 software system build), any breach that alters data values cannot be attested during a forensic audit. Each voter record transaction update results in overwriting not recording the previous input. In Oct of 2023, the SoS CISO Jillian Burner acknowledged as much. Security controls for voter registration databases need to be brought up to 2024 standards leveraging blockchain digital ledger along with other zero trust security controls similar to the 16 other designated "critical infrastructure" sectors.

https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers/

States notified by DHS of Russian hacking attempts



Source: News reports and public statements

THE FIX

Biggest Issues for Ohio's and Nations Voting Systems

- There is a very low level of security standards used to develop voting systems, case in point, all voting machines, markers and tabulators for the 2024 general election were certified to a VVSG 1.0 (2005) security standard, our current State law states those certifications need to be "to the most up to date VVSG" standard, they are not!
- Moreover, there is very limited visibility into voting system development practices software design & production
- To date, no requirements are imposed on voting system vendors to disclose their foreign ownership or personnel policies and procedures related to the conduct of background checks intended to safeguard against insider threats
- Also, there are no requirements for voting system vendors to disclose supply chain parts, patches and origin of installations, nor how they are transported and how they are kept secure
- While Ohio law and the SoS BVSE base State certification on federal certification of voting machines, markers and tabulators, all other election products and services in use in Ohio to include Voter Registration Databases, E-Pollbooks and Election Night Reporting Services are NOT certified to cybersecurity standards
- The bottom-line and concerning disconnect is voting system vendors-unlike vendors in other critical infrastructure sectors such as defense-face almost no federal or State oversight of their security systems before they are procured and fielded by State election officials. In the Air Force, we would refer to this oversight as flying blind.
    - Ohio SoS's efforts to mandate intrusion detection network monitoring services through non-profit Center for Internet Security via DHS/CISA funded contract grants CANNOT solve for or mitigate security breaches to voting system devices, databases or software application for UNKNOWN threats. Ohio's voting systems have yet to meet the full complement of NIST Cybersecurity Framework Core Functions of (Identify, Protect, Detect, Respond, Recover)

Impact: Establishing trust around the integrity of data stored in database systems has been a longstanding problem going back to the 2005 period upon which these databases began their current use

- There is no denying that voter registration databases are vulnerable
    - The Senate Select Intelligence Committee issued an authoritative report in 2019 that up to 7 State Voter Registration databases were accessed by unauthorized users with data breached and stolen in the 2016 election
    - Since that period an additional five States have experienced data breaches, exploitation and potential alteration of data which cannot be forensically evaluated because the manner is which the data is stored in these databases is not able to playback transactions changes.
    - By incorporating blockchain digital ledger on top of existing SQL databases, Ohio would be the 1st state to adopt a tamper resistance and evidence based capability when unauthorized access or alteration takes place
    - Blockchain functionality in the Voter Registration database preserves voter record data in a co-located history table that enables a cost-effective and streamlined audit retrieval capability to fully recover and restore data alterations
    - Security controls in blockchain include group validation and consensus mechanisms for voter record changes reducing the risk of malicious alteration
    - Additionally all data values and transactions, utilize cryptographic security controls and multi-factor authentication for verification, bringing critical infrastructure voting systems up to financial and crypto industry standards.

Conclusion: Ohio's legislature must act now to reduce the attack spectrum to our voting systems, establish data integrity and trust to our voter registration databases through blockchain digital ledger adoption with enhanced security controls and require critical voter registration identity data validation and verification to prevent non-citizens and ineligible persons from registering in the first place and voting illegally.

Let me know if you have questions.

-Marcell Strbich
Ohio Election Study Collaborative
Sent with Proton Mail secure email.

Hannum, Logan

From: mstrbic <mstrbic@protonmail.com>
Sent: Monday, March 25, 2024 12:15 AM
To: Willis, Bernard
Cc: Gail Niederlehner; Jim Rigano; swiggam@gmail.com
Subject: Fw: Buckeye Institute Introduction to Ohio Election Bill
Attachments: Executive Summary_Ohio Votes Count Act_Mar 24.pdf; BMV FOIA Request Valid Identities issued to Non-Citizens_2024.docx; FOIA to SOS for 2023 info on Annual Non-Citizen Audit of Statewide Voter File Database.docx

Representative Willis,

Senior Legal Fellow of Conservative Partnership Institute (CPI) Cleta Micthell has come out strong for the proposed Ohio Votes Count Act. She offered to broker an introduction to the Buckeye Institute President Robert Alt for bill proponency.

Support of the election bill from the States foremost conservative affiliated think tank would lend further credibility to legislators considering co-sponsorship should they take a public position or testify on the bill.

Please feel free to share this development with the Committee Chairman.

Thank you,
Marcell Strbich
Ohio Elections Study Collaborative

Sent with Proton Mail secure email.

------- Forwarded Message -------
From: mstrbic <mstrbic@protonmail.com>
Date: On Sunday, March 24th, 2024 at 11:55 PM
Subject: Buckeye Institute Introduction to Ohio Election Bill
To: Cleta Mitchell <cleta@cletamitchell.com>
CC: Bryson Davis <bryson@electionintegrity.network>, Eileen Watts <ewattsohio@gmail.com>, Jim Womack <james.k.womack@gmail.com>, Barry Chapman <bchapman@cox.net>, Gail Niederlehner <ohio4truth@proton.me>, Jim Rigano <jim@rigano.net>, Eileen Watts <ewatts@columbus.rr.com>, ws095@hotmail.com <ws095@hotmail.com>

Hi Cleta,

Great idea! Could you please broker an introduction to Robert Alt of the Buckeye Institute to myself, Eileen Watts, and former Ohio legislator advisor Bill Schuck? Would a conference call sometime this week be possible?

Our objectives for the meeting involve introducing the following-

- Highlights of OH's citizen-initiated pending election bill (Exec Summary Attached)
  - Existing OH voter registration verification and data validation deficiencies
  - Overview of voting system certification standards, State non-compliance & security deficiencies
- BMV disclosed findings on non-citizens possessing OH voter credentials (Attached)

- Pending SoS FOIA request for 2023 annual non-citizen audit results of Statewide Registration Database (Attached)

We really could benefit from partnering with the renowned Buckeye Institute for legal support, advise and advocacy in the coming weeks as multiple legislative and potential legal filings coalesce leading up to the 2024 election.

Thank you,
Marcell Strbich

Sent with Proton Mail secure email.

On Sunday, March 24th, 2024 at 7:15 AM, Cleta Mitchell <cleta@cletamitchell.com> wrote:

Oh wow! That's phenomenal!!

Your data about noncitizens - have you petitioned the SOS to remove those registrations specifically and submitted with documentation of noncitizen status?

Have you considered reaching out to Robert Alt at Buckeye Institute to represent the coalition and file suit to remove these and other new noncitizens asap?

I'd be happy to connect you with Robert. Let me know. Cleta

Cleta Mitchell, Esq.
Senior Legal Fellow
Conservative Partnership Institute
202.431.1950 (cell)
cleta@cletamitchell.com
www.whoscounting.us

On Mar 23, 2024, at 10:16 PM, mstrbic <mstrbic@protonmail.com> wrote:

Hi Cleta,

We'll definitely look to bring Ralph onboard. To answer your question, our efforts (OEIN) are independent of the United Sovereign Americans (USA); however, the provisions within our proposed election bill would solve many of the voter registration inaccuracies and subsequent registration and voting violations alleged in the complaint.

I've attached a 1-pg Executive Summary of a constituent written election bill that will drop in Ohio's House in early Apr. The Chairman of Government Oversight Accountability Committee Rep Bob Peterson agreed to co-sponsor with Rep Berni Willis. Both State House Speaker and Senate President were apprised and receptive to bringing this election bill to a full vote in legislature when ready.

Of note, the bill proposes multiple 1st-in-the nation measures-

- State-directed independent 3rd party cyber security assessment reviews of voting systems as condition of certification in addition to EAC VVSG 2.0 standards

- Defined voting system certification standards based on most up to date federal software security development guidelines to include vendor voting system disclosure requirements

- Independent audits of Voter Registration Databases by Auditor of State

- Adoption of anti-tamper proof digital blockchain ledger functionality for Voter Registration Databases at both State and County level

- Voter registration data validation measures and identity and citizenship verification PRIOR to SoS acceptance on voter rolls (i.e. Not being done today – 267K+ illegals in Ohio)

- County opt-in provision for hand counted paper ballots in place of voting machines.

If you or other stakeholders are interested, we can provide a presentation.

Let me know.

Marcell Strbich
Ohio Election Research Collaborative (OEIN Affiliate)

Sent with Proton Mail secure email

Sent with Proton Mail secure email.

On Sunday, March 24th, 2024 at 7:15 AM, Cleta Mitchell <cleta@cletamitchell.com> wrote:

> Oh wow! That's phenomenal!!
>
> Your data about noncitizens - have you petitioned the SOS to remove those registrations specifically and submitted with documentation of noncitizen status?
>
> Have you considered reaching out to Robert Alt at Buckeye Institute to represent the coalition and file suit to remove these and other new noncitizens asap?
>
> I'd be happy to connect you with Robert. Let me know. Cleta
>
> Cleta Mitchell, Esq.
> Senior Legal Fellow
> Conservative Partnership Institute
> 202.431.1950 (cell)
> cleta@cletamitchell.com
> www.whoscounting.us
>
> > On Mar 23, 2024, at 10:16 PM, mstrbic <mstrbic@protonmail.com> wrote:
> >
> > Hi Cleta,
> >
> > We'll definitely look to bring Ralph onboard. To answer your question, our efforts (OEIN) are independent of the United Sovereign Americans (USA); however, the provisions within our proposed election bill would solve many of the voter registration inaccuracies and subsequent registration and voting violations alleged in the complaint.
> >
> > I've attached a 1-pg Executive Summary of a constituent written election bill that will drop in Ohio's House in early Apr. The Chairman of

Government Oversight Accountability Committee Rep Bob Peterson agreed to co-sponsor with Rep Berni Willis. Both State House Speaker and Senate President were apprised and receptive to bringing this election bill to a full vote in legislature when ready.

Of note, the bill proposes multiple 1st-in-the nation measures-

- State-directed independent 3rd party cyber security assessment reviews of voting systems as condition of certification in addition to EAC VVSG 2.0 standards

- Defined voting system certification standards based on most up to date federal software security development guidelines to include vendor voting system disclosure requirements

- Independent audits of Voter Registration Databases by Auditor of State

- Adoption of anti-tamper proof digital blockchain ledger functionality for Voter Registration Databases at both State and County level

- Voter registration data validation measures and identity and citizenship verification PRIOR to SoS acceptance on voter rolls (i.e. Not being done today – 267K+ illegals in Ohio)

- County opt-in provision for hand counted paper ballots in place of voting machines.

If you or other stakeholders are interested, we can provide a presentation.

Let me know.

Marcell Strbich
Ohio Election Research Collaborative (OEIN Affiliate)

Sent with Proton Mail secure email.

From: Allison Crisci-Nickolai <allisonnickolai@msn.com>
Sent: Sunday, March 24, 2024 9:35 PM
To: jpayne@dps.ohio.gov <jpayne@dps.ohio.gov>
Subject: Re: Request for information!

BMV information requested for 2024

From: Allison Crisci-Nickolai <allisonnickolai@msn.com>
Sent: Thursday, March 7, 2024 6:12 PM
To: jpayne@dps.ohio.gov <jpayne@dps.ohio.gov>
Subject: Request for information!

I hope this finds you well and busy, but I hope you can take a moment to provide me with the following information for 2024.
I am hoping the data I am requesting will coincide with the request from the Elections division to conduct the Annual Non Citizen Audit of the voter rolls..

1. How many valid Driver's licenses and State issued ID's are currently in circulation in Ohio?
2. How many valid Driver's licenses and State Issued ID's are currently issued to NON CITIZENS in Ohio?

I have a couple additional questions about access to the BMV database used by Job and Family Services.

1) is the level of access to the BMV by JFS sufficient to determine citizenship of an applicant for programs IF the applicant provides a state issued DL or ID?

2) Is the Level of access to BMV (by JFS) sufficient to determine if any credential is still valid in the State of Ohio? (Meaning, the DL has not been transferred to another state due to a relocation?)

It is my understanding that the Ohio credential is invalidated once an application for a DL has been accepted and a credential issued by another state. Is that correct?

Thank you in advance. Your responses are greatly appreciated and help me understand the process so I can educate others,

Allison Nickolai

Sent to SOS for 2023 information

From: Allison Crisci-Nickolai <allisonnickolai@msn.com>
Sent: Thursday, March 7, 2024 4:09 PM
To: Warren, Sally <SWarren@OhioSOS.Gov>
Subject: Fw: 2023 Annual Citizenship Audit Request for information

To date I have received no notice my request was received. Can you help please?

TIA
Allison Nickolai

From: Allison Crisci-Nickolai <allisonnickolai@msn.com>
Sent: Wednesday, February 28, 2024 12:37 PM
To: election@ohiosos.gov <election@Ohiosos.gov>
Subject: 2023 Annual Citizenship Audit Request for information

Dear Ohio Board of Elections

This is a request for records under the Open Records Law (Ohio Rev. Code sec, 149.43 et seq,)
I respectfully request that you make available to me the following records and reports::

1. The number of REPORTED registrations identified by the 2023 Annual Non Citizen Audit of the Statewide Voter File Database (SWVFDB) that is lawfully conducted per ORC- Section 3503.152 Review of database for noncitizens
    a. This should be the initial amount of registrations identified
2. The number of Reported registrations NOT submitted to County Boards of Elections for follow up (the number removed from consideration, if any)
3. The number of researched registrations sent to county Boards of Elections for mailing of the Ohio Registration Eligibility Confirmation form RC 3503.15(H) and accompanying letter from SoS
4. The total number of NON RESPONSES reported back to the SoS from the above mailings by the county BOE's.

5. The total number of registrations that were referred to AG Dave Yost for prosecution in 2023.

6. The total number of non citizen registrations removed as a result of the Annual Non Citizen Audit conducted in 2023.

I am not requesting individual records or any Personally Identifiable Information for any of the record information above, so the numbers of registrations should be straight forward from any report generated. This information will be used to assist with public education on this audit process and with drafting of legislation on the effectiveness of the annual Non Citizen Audit process already in progress with LSC.

Also: Who can review the actual ORC stated above (printed below) for the following apparent discrepancy?

"(A) The secretary of state shall compare the information in the statewide voter registration database with the information the secretary of state obtains from the bureau of motor vehicles under section 3503.151 of the Revised Code to identify any person who does all of the following, in the following order:

(1) Submits documentation to the bureau of motor vehicles that indicates that the person is not a United States citizen;

(2) Registers to vote, submits a voter registration change of residence or change of name form, or votes in this state;

(3) Submits documentation to the bureau of motor vehicles that indicates that the person is not a United States citizen.

It appears that item 1 and Item 3 are exactly the same, and cannot be sequentially processed as (A) states as the documentation would already be on file with BMV and the voter would not be eligible to enter the voter rolls if

properly researched at registration. Can someone at the board of elections contact me to discuss or explain this please? TIA

Any and all relevant information and reports responding to the above records request can be submitted electronically.
Thank you in Advance

Allison M. Nickolai
937-570-1197
allisonnickolai@msn.com

Summary HB XX - Ohio Votes Count Act

Big Picture Issues

- Elec on officials are not computer specialists, but elec ons rely heavily on computer technology.
- Even when known to be ineligible, a voter registra on generally requires 4 or more years to be removed.
- Vo ng systems are built and cer fied to outdated 2005 security standards.
- Ohio elec ons lack safeguards to prevent 267,000+ non-ci zens from registering and vo ng.

Voter Registration Data Validation

ISSUES: State and county voter registra on systems contain numerous avoidable data entry errors.

SOLUTIONS:

- Use reference lists of names and addresses to verify new and exis ng voter registra on records.
- Issue weekly reports to coun es iden fying various errors in their voter registra on databases.
- Before adding an applicant to the voter registra on database, require the voter registra on to match the informa on on the applicant's driver's license or state id card.
- Cancel voter registra ons for electors who have moved if they are registered to vote or have applied for a driver's license in another state.
- Simplify the system for assigning unique record iden fiers in the statewide voter registra on database.
- Use a commercial service for monthly voter registra on data analysis.

Audit Voter Registration Databases

ISSUES: The current audit is not independent or thorough.

SOLUTIONS:

- Require the Auditor of State to conduct an annual audit of the statewide voter registra on database and three randomly selected coun es.

Identity and Citizenship Verification

ISSUES: There are insufficient safeguards to prevent nonci zens and ineligible persons from registering and vo ng.

SOLUTIONS:

- Increase the frequency of review for non-ci zens and other ineligible voters.
- Provide coun es with resources to verify iden ty and ci zenship prior to registra on and for absentee and provisional ballot screening.
- Expand voter registra on instruc ons to include ci zenship and other eligibility requirements.
- Introduce safeguards and procedures at social services, BMV and registra on agencies to ensure nonci zens are not misled into illegally registering to vote.
- Require an elector to vote a provisional ballot un l US ci zenship is verified.

Board of Voting System Examiners

ISSUES: The Board lacks cybersecurity exper se and cer fica on standards for voter registra on systems.

SOLUTIONS:

- Include cybersecurity experts on the board of vo ng system examiners.
- Establish standards and require cer fica on of new voter registra on systems.
- Cybersecurity review is necessary to cer fy a new vo ng system.
- Require publica on of vo ng system cer fica on reports and recommenda ons.
- Require voter registra on systems to be physically located in Ohio in a facility under the board of elec ons control.

Cybersecurity Standards

ISSUES: Elec on systems security standards are outdated.

SOLUTIONS:

- Use 3rd party reviewers to conduct a cyber security assessment of vo ng systems seeking cer fica on.
- Adopt vo ng system cer fica on standards based on most recent NIST and current federal guidelines.
- Require a periodic review and vo ng system vendor disclosure of so ware development prac ces as part of a con nued cer fica on security review.
- Require use of a digital blockchain ledger to log all voter registra on system changes.

County Voting System Backup

ISSUES: No con ngencies exist if a vo ng system is decer fied.

SOLUTIONS:

- Authorize a county opt-in provision for hand counted paper ballots through passage of an electorate introduced ballot pe on ini a ve.

Election Administration

- ☐ Requires an elector to sign a form when upda ng their voter registra on.
- ☐ Requires publishing of elec on reports to the internet.
- ☐ Ins tutes a procedure to follow when voter registra on acknowledgement forms are not returned.
- ☐ Requires mail-in voters to include a copy of their voter iden fica on when returning their absentee ballot.
- ☐ Requires a provisional ballot to be counted when both a provisional and absentee ballot are cast.

Hannum, Logan

From: Willis, Bernard
Sent: Monday, March 25, 2024 4:13 PM
To: mstrbic
Cc: Gail Niederlehner; Jim Rigano; swiggam@gmail.com; Hannum, Logan; Peterson, Bob
Subject: Re: Buckeye Institute Introduction to Ohio Election Bill

I love it. Let's get together with them soon. Maybe we can set up a F2F meet after Easter?

Bunyan

Get Outlook for iOS

From: mstrbic <mstrbic@protonmail.com>
Sent: Sunday, March 24, 2024 10:19 PM
To: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Cc: Gail Niederlehner <ohio4truth@proton.me>; Jim Rigano <jim@rigano.net>; swiggam@gmail.com <swiggam@gmail.com>
Subject: Fw: Buckeye Institute Introduction to Ohio Election Bill

Representative Willis,

Senior Legal Fellow of Conservative Partnership Institute (CPI) Cleta Micthell has come out strong for the proposed Ohio Votes Count Act. She offered to broker an introduction to the Buckeye Institute President Robert Alt for bill proponency.

Support of the election bill from the States foremost conservative affiliated think tank would lend further credibility to legislators considering co-sponsorship should they take a public position or testify on the bill.

Please feel free to share this development with the Committee Chairman.

Thank you,
Marcell Strbich
Ohio Elections Study Collaborative

Sent with Proton Mail secure email.

------- Forwarded Message -------
From: mstrbic <mstrbic@protonmail.com>
Date: On Sunday, March 24th, 2024 at 11:55 PM
Subject: Buckeye Institute Introduction to Ohio Election Bill
To: Cleta Mitchell <cleta@cletamitchell.com>
CC: Bryson Davis <bryson@electionintegrity.network>, Eileen Watts <ewattsohio@gmail.com>, Jim Womack <james.k.womack@gmail.com>, Barry Chapman <bchapman@cox.net>, Gail Niederlehner <ohio4truth@proton.me>, Jim Rigano <jim@rigano.net>, Eileen Watts <ewatts@columbus.rr.com>, ws095@hotmail.com <ws095@hotmail.com>

Hi Cleta,

Great idea! Could you please broker an introduction to Robert Alt of the Buckeye Institute to myself, Eileen Watts, and former Ohio legislator advisor Bill Schuck? Would a conference call sometime this week be possible?

Our objectives for the meeting involve introducing the following-

- Highlights of OH's citizen-initiated pending election bill (Exec Summary Attached)
  - Existing OH voter registration verification and data validation deficiencies
  - Overview of voting system certification standards, State non-compliance & security deficiencies
- BMV disclosed findings on non-citizens possessing OH voter credentials (Attached)
- Pending SoS FOIA request for 2023 annual non-citizen audit results of Statewide Registration Database (Attached)

We really could benefit from partnering with the renowned Buckeye Institute for legal support, advise and advocacy in the coming weeks as multiple legislative and potential legal filings coalesce leading up to the 2024 election.

Thank you,
Marcell Strbich

Sent with Proton Mail secure email.

On Sunday, March 24th, 2024 at 7:15 AM, Cleta Mitchell <cleta@cletamitchell.com> wrote:

Oh wow! That's phenomenal!!

Your data about noncitizens - have you petitioned the SOS to remove those registrations specifically and submitted with documentation of noncitizen status?

Have you considered reaching out to Robert Alt at Buckeye Institute to represent the coalition and file suit to remove these and other new noncitizens asap?

I'd be happy to connect you with Robert. Let me know. Cleta

Cleta Mitchell, Esq.
Senior Legal Fellow
Conservative Partnership Institute

202.431.1950 (cell)
cleta@cletamitchell.com
www.whoscounting.us

On Mar 23, 2024, at 10:16 PM, mstrbic <mstrbic@protonmail.com> wrote:

Hi Cleta,

We'll definitely look to bring Ralph onboard. To answer your question, our efforts (OEIN) are independent of the United Sovereign Americans (USA); however, the provisions within our proposed election bill would solve many of the voter registration inaccuracies and subsequent registration and voting violations alleged in the complaint.

I've attached a 1-pg Executive Summary of a constituent written election bill that will drop in Ohio's House in early Apr. The Chairman of Government Oversight Accountability Committee Rep Bob Peterson agreed to co-sponsor with Rep Berni Willis. Both State House Speaker and Senate

President were apprised and receptive to bringing this election bill to a full vote in legislature when ready.

Of note, the bill proposes multiple 1st-in-the nation measures-

- State-directed independent 3rd party cyber security assessment reviews of voting systems as condition of certification in addition to EAC VVSG 2.0 standards

- Defined voting system certification standards based on most up to date federal software security development guidelines to include vendor voting system disclosure requirements

- Independent audits of Voter Registration Databases by Auditor of State

- Adoption of anti-tamper proof digital blockchain ledger functionality for Voter Registration Databases at both State and County level

- Voter registration data validation measures and identity and citizenship verification PRIOR to SoS acceptance on voter rolls (i.e. Not being done today – 267K+ illegals in Ohio)

- County opt-in provision for hand counted paper ballots in place of voting machines.

If you or other stakeholders are interested, we can provide a presentation.

Let me know.

Marcell Strbich
Ohio Election Research Collaborative (OEIN Affiliate)

Sent with Proton Mail secure email

Sent with Proton Mail secure email.

On Sunday, March 24th, 2024 at 7:15 AM, Cleta Mitchell <cleta@cletamitchell.com> wrote:

> Oh wow! That's phenomenal!!
>
> Your data about noncitizens - have you petitioned the SOS to remove those registrations specifically and submitted with documentation of noncitizen status?
>
> Have you considered reaching out to Robert Alt at Buckeye Institute to represent the coalition and file suit to remove these and other new noncitizens asap?
>
> I'd be happy to connect you with Robert. Let me know. Cleta
>
> Cleta Mitchell, Esq.
> Senior Legal Fellow
> Conservative Partnership Institute
>
> 202.431.1950 (cell)
> cleta@cletamitchell.com
> www.whoscounting.us

On Mar 23, 2024, at 10:16 PM, mstrbic <mstrbic@protonmail.com> wrote:

Hi Cleta,

We'll definitely look to bring Ralph onboard. To answer your question, our efforts (OEIN) are independent of the United Sovereign Americans (USA); however, the provisions within our proposed election bill would solve many of the voter registration inaccuracies and subsequent registration and voting violations alleged in the complaint.

I've attached a 1-pg Executive Summary of a constituent written election bill that will drop in Ohio's House in early Apr. The Chairman of Government Oversight Accountability Committee Rep Bob Peterson agreed to co-sponsor with Rep Berni Willis. Both State House Speaker and Senate President were apprised and receptive to bringing this election bill to a full vote in legislature when ready.

Of note, the bill proposes multiple 1st-in-the nation measures-

- State-directed independent 3rd party cyber security assessment reviews of voting systems as condition of certification in addition to EAC VVSG 2.0 standards

- Defined voting system certification standards based on most up to date federal software security development guidelines to include vendor voting system disclosure requirements

- Independent audits of Voter Registration Databases by Auditor of State

- Adoption of anti-tamper proof digital blockchain ledger functionality for Voter Registration Databases at both State and County level

- Voter registration data validation measures and identity and citizenship verification PRIOR to SoS acceptance on voter rolls (i.e. Not being done today – 267K+ illegals in Ohio)

- County opt-in provision for hand counted paper ballots in place of voting machines.

If you or other stakeholders are interested, we can provide a presentation.

Let me know.

Marcell Strbich
Ohio Election Research Collaborative (OEIN Affiliate)

Sent with Proton Mail secure email.

Hannum, Logan

From: Eileen Watts <ewattsohio@gmail.com>
Sent: Monday, May 20, 2024 12:48 PM
To: State Senator Theresa Gavarone; State Senator Andrew Brenner; Willis, Bernard; Rep Bernie Willis; Peterson, Bob
Cc: Marcell Strbich; Gail Niederlehner; Jim Rigano
Subject: Meeting to Brief on HB 472

Ohio Election Integrity Network is inviting you to a scheduled Zoom meeting.

Topic: HB 472 briefing for Senators
Time: May 20, 2024 01:00 PM Eastern Time (US and Canada)

Join Zoom Meeting
https://zoom.us/j/95895789585?pwd=OXVIQjB0WnNuRmdNSStneDB5ZENNUT09

Meeting ID: 958 9578 9585
Passcode: 930912

One tap mobile
+13126266799,,95895789585#,,,,*930912# US (Chicago)
+16469313860,,95895789585#,,,,*930912# US

Dial by your location
- **+1 312 626 6799 US (Chicago)**
- **+1 646 931 3860 US**
- **+1 929 436 2866 US (New York)**
- **+1 301 715 8592 US (Washington DC)**
- **+1 305 224 1968 US**
- **+1 309 205 3325 US**
- **+1 689 278 1000 US**
- **+1 719 359 4580 US**
- **+1 253 205 0468 US**
- **+1 253 215 8782 US (Tacoma)**
- **+1 346 248 7799 US (Houston)**
- **+1 360 209 5623 US**
- **+1 386 347 5053 US**
- **+1 507 473 4847 US**
- **+1 564 217 2000 US**
- **+1 669 444 9171 US**
- **+1 669 900 6833 US (San Jose)**

Meeting ID: 958 9578 9585
Passcode: 930912

Find your local number: https://zoom.us/u/ah46AKgdL

Eileen Watts
ewattsohio@gmail.com
614-352-1010

Hannum, Logan

From: mstrbic <mstrbic@protonmail.com>
Sent: Monday, May 20, 2024 2:23 PM
To: Eileen Watts
Cc: State Senator Theresa Gavarone; State Senator Andrew Brenner; Willis, Bernard; Rep Bernie Willis; Peterson, Bob; Gail Niederlehner; Jim Rigano
Subject: Re: Meeting to Brief on HB 472 (Election Cybersecurity Bill)
Attachments: Securing Ohios Election Infrastucture_sept 2023.pdf; Securing OHs Voter Registration Systems_Oct 30th 2023.pdf

ALCON,

Please see the attached and preceding presentations prepared on your behalf in advance of your consideration for sponsorship of this critical election security legislation.

- Attachment #1: Securing Ohio's Election Infrastructure (3rd Party Security Reviews)
- Attachment #2: Securing Ohio's Voter Registration Systems (Blockchain)

Both presentations were given to the OH SoS and House Members in advance of legislative sponsorship of H.B. 472 The Ohio Votes Count Act (3 Apr 2024). Proponent testimony is scheduled this Wed (22 May/1100) in the House Homeland Security Committee chaired by Rep Haraz Ghanbari.

Thank you,
Marcell Strbich

Sent with Proton Mail secure email.

On Monday, May 20th, 2024 at 12:47 PM, Eileen Watts <ewattsohio@gmail.com> wrote:

> **Ohio Election Integrity Network is inviting you to a scheduled Zoom meeting.**
>
> **Topic: HB 472 briefing for Senators**
> **Time: May 20, 2024 01:00 PM Eastern Time (US and Canada)**
>
> **Join Zoom Meeting**
> **https://zoom.us/j/95895789585?pwd=OXVIQjB0WnNuRmdNSStneDB5ZENNUT09**
>
> **Meeting ID: 958 9578 9585**
> **Passcode: 930912**
>
> ---
>
> **One tap mobile**
> **+13126266799,,95895789585#,,,,*930912# US (Chicago)**
> **+16469313860,,95895789585#,,,,*930912# US**
>
> ---

Dial by your location
- +1 312 626 6799 US (Chicago)
- +1 646 931 3860 US
- +1 929 436 2866 US (New York)
- +1 301 715 8592 US (Washington DC)
- +1 305 224 1968 US
- +1 309 205 3325 US
- +1 689 278 1000 US
- +1 719 359 4580 US
- +1 253 205 0468 US
- +1 253 215 8782 US (Tacoma)
- +1 346 248 7799 US (Houston)
- +1 360 209 5623 US
- +1 386 347 5053 US
- +1 507 473 4847 US
- +1 564 217 2000 US
- +1 669 444 9171 US
- +1 669 900 6833 US (San Jose)

Meeting ID: 958 9578 9585
Passcode: 930912

Find your local number: https://zoom.us/u/ah46AKgdL

Eileen Watts
ewattsohio@gmail.com
614-352-1010

Securing Ohio's Election Infrastructure

A Legislative Approach and Cyber Security Perspective

Ohio Election Study Collaborative

Presenter: Marcell Strbich

September 8thth 2023

The views expressed are those of the individual only and not those of the U.S. Air Force or Dept of Defense

Overview

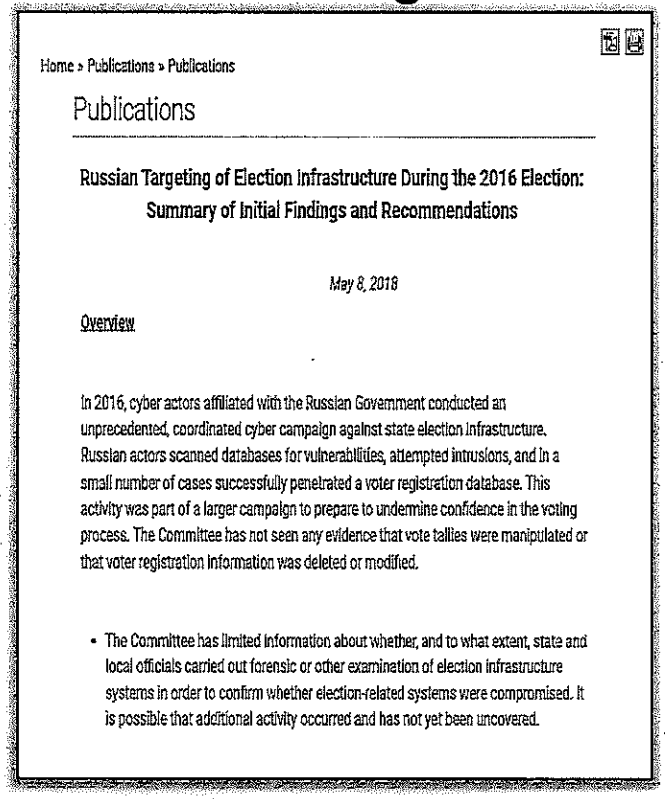
- Assessing Security Risk to Election Infrastructure
  - EO 14028 Improving the Nation's Cybersecurity
  - Election "Critical" Infrastructure Overview
  - Vendor – Products and Services Overview
- Federal Testing & Certification Process – The Problem
  - Voting System Certification – Issues & Challenges
  - Ohio Law Disconnect with Federal Law
- Current Ohio Election Security Measures – The Gap
  - Cybersecurity Functions Framework
  - Wireless Network Configuration – Patent Example
  - Current Law Vs. Standard – Election Systems
- Threats to Auditability - Ohio Use Case (DREs)
  - Computerized Voting Systems – Security Vulnerabilities
- National Resolution – Republican National Committee
  - Election Infrastructure – Cost Benefit Analysis
  - Ohio County BOE Engagement – Committee Report
  - Greene County – Opposing Resolution on DREs
  - Opt-Out Clause – Criteria & Alternatives
- Ohio Voting System Certification – The Solution
  - *Revised Ohio Law Security – Certification Provisions*
  - Vendor Certifiability – Requirement Standards
  - Summary – Recap and Questions

Assessing Security Risk to Election Infrastructure

Private Vendors play a central role in American elections ~ Prime Target

U.S. Senate Intelligence Committee Report (2018)

Publications | Intelligence Committee (senate.gov) –
Russian Targeting of Election Infrastructure



Home » Publications » Publications

Publications

Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations

May 8, 2018

Overview

In 2016, cyber actors affiliated with the Russian Government conducted an unprecedented, coordinated cyber campaign against state election infrastructure. Russian actors scanned databases for vulnerabilities, attempted intrusions, and in a small number of cases successfully penetrated a voter registration database. This activity was part of a larger campaign to prepare to undermine confidence in the voting process. The Committee has not seen any evidence that vote tallies were manipulated or that voter registration information was deleted or modified.

- The Committee has limited information about whether, and to what extent, state and local officials carried out forensic or other examination of election infrastructure systems in order to confirm whether election-related systems were compromised. It is possible that additional activity occurred and has not yet been uncovered.

Key Takeaway:

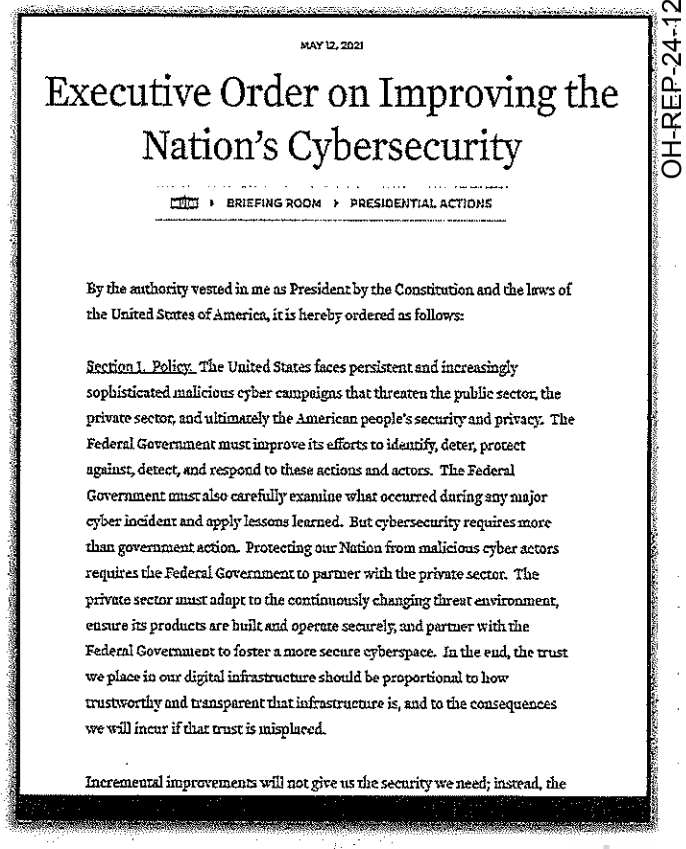
"State local, territorial, tribal, and federal government authorities have very little insight into the cyber security practices of [election] vendors"

Impossible to assess risk to vendors or impact to election security Without risk management framework

Executive Order 14028 – Improving the Nation's Cybersecurity (2021)

Key Highlights: Enhanced Vendor Risk Assessments

- **Growing emphasis on software security in supply chains**
- **Creates *higher standards for software verification techniques*** and other software ***supply chain controls***
- **Perform additional scrutiny on vendor Software Development Lifecycle (SDLC) capabilities,** security posture, and risks associated with Foreign Ownership, Control, or Influence (FOCI)



MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM › PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

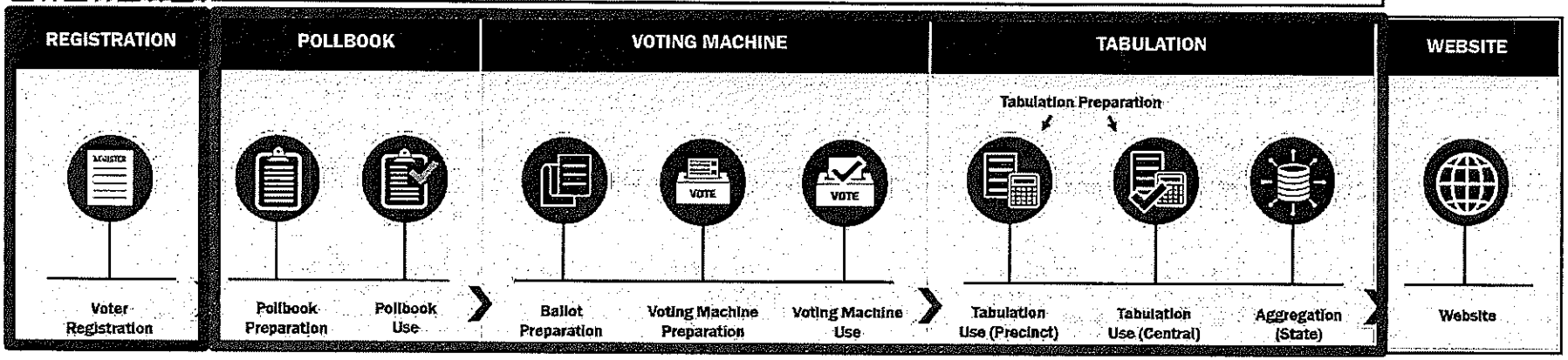
Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the

Federal government placing additional scrutiny on the software that vendors produce

Election "Critical" Infrastructure Overview

S.B. 14 Current scope of OH ***Board of Voting Machine Examiners*** **equipment approval**



Who has oversight of election vendors and authority to certify?

Where's the Critical Gap?

LIMITED TRANSPARENCY & ACCOUNTABILITY INTO VENDOR-DEVELOPER SECURITY PRACTICES

Ohio has opportunity to empower a State level Cyber security review team to conduct system security design and vulnerability verification

Vendor - Products and Services Overview

Vendors Present Points of Attack into Election Infrastructure

Voter Registration Database - No Federal or State certification standard

Voter registration info is housed in statewide databases that in many jurisdictions are created or maintained by a vendor.

Ballot Programming - No Federal or State certification standard

Prior to every election, voting machines must be programmed with a memory card or USB stick to display the ballot or read and count votes. Vendors provide the software.

Electronic Pollbooks – No Federal or State certification standard

On Election Day, poll workers in jurisdictions checking in voters using electronic pollbooks, usually provided by a vendor.

Voting Systems – Only partial voluntary certification standards at federal level

Jurisdictions use a variety of voting machines, all provided by vendors.

Election Night Reporting - No Federal or State certification standard

On election night, the general public can view election results through reporting websites provided by vendors.

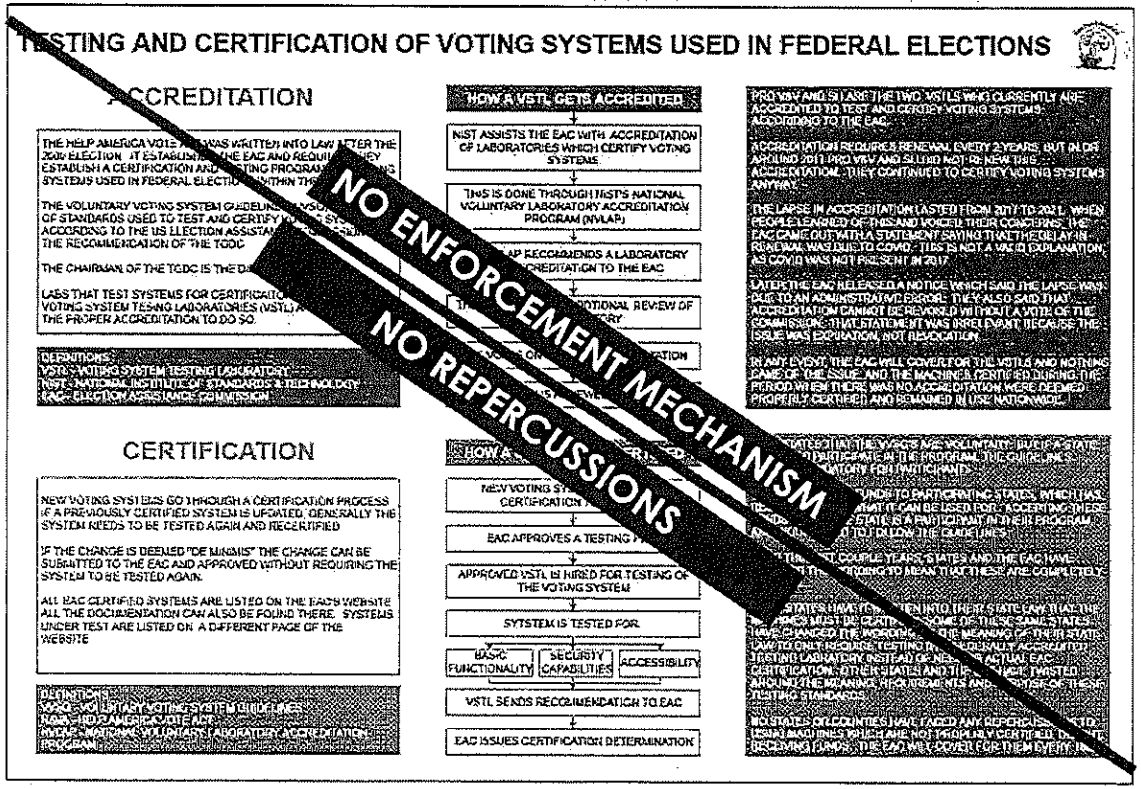
Postelection Audits - No Federal or State certification standard

After an election, vendors and their equipment play a role in checking that the equipment and procedures used to count votes worked properly and that the election yielded the correct results.

Ohio law for voting machine certification based on federal voluntary guidelines

Federal Testing & Certification Process – The Problem

Federal Election Assistance Commission (EAC)



Questionable Vendor Affiliation Influence

Only 2 National Voting System Labs

- Pro V&V & SLI
- Tests biased by manufacturer design, influence and funding

Test Objectivity & Oversight Deficit

- EAC lab accreditation delinquent 2017-2021
  - ***Voting systems still being certified to 2005 security standards (VVSG 1.0)***
  - Problems in multiple states (VA, NC, AZ)
  - No independent vendor cybersecurity attestation as criteria for certification

EAC does not have statutory authority to certify most election vendors

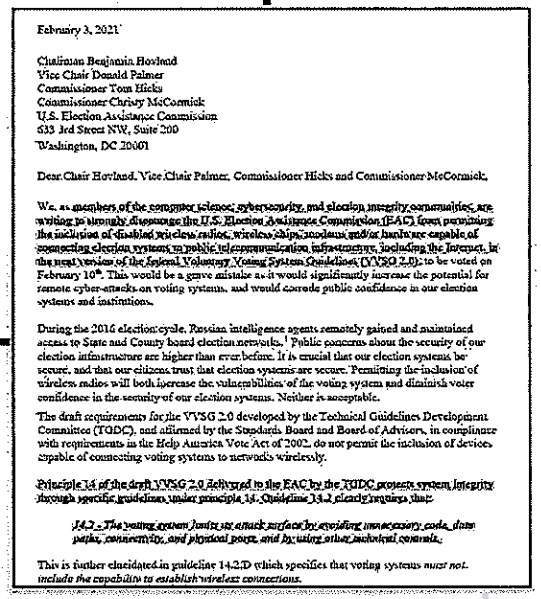
Voting System Certification Issues & Challenges

Computerized Voting System Security Vulnerabilities

EAC VVSG 2.0 standards will NOT mitigate ***known remote access threat***

25 leading computer science, cybersecurity & election integrity communities experts objected **to EAC inclusion of *disabled wireless radio, wireless chips, modems and/or hardware*** *capable* of connecting election systems to public telecom infrastructure in ***Voluntary Voting System Guidelines (VVSG 2.0)***

VVSG 2.0 Approval objection letter to Election Assistance Commission



February 3, 2021

Chairman Benjamin Hovland
Vice Chair Donald Palmer
Commissioner Tom Hicks
Commissioner Christy McCormick
U.S. Election Assistance Commission
633 3rd Street NW, Suite 200
Washington, DC 20001

Dear Chair Hovland, Vice Chair Palmer, Commissioner Hicks and Commissioner McCormick,

We, as members of the computer science, cybersecurity, and election integrity communities, are writing to strongly discourage the U.S. Election Assistance Commission (EAC) from permitting the inclusion of disabled wireless radios, wireless chips, modems, and/or hardware capable of connecting election systems to public telecommunication infrastructure, including the Internet, in the next version of the federal Voluntary Voting System Guidelines (VVSG 2.0), to be voted on February 10th. This would be a grave mistake as it would significantly increase the potential for remote cyber-attacks on voting systems, and would corrode public confidence in our election systems and institutions.

During the 2016 election cycle, Russian intelligence agents remotely gained and maintained access to State and County board election networks.[1] Public concerns about the security of our election infrastructure are higher than ever before. It is crucial that our election systems be secure, and that our citizens trust that election systems are secure. Permitting the inclusion of wireless radios will both increase the vulnerabilities of the voting system and diminish voter confidence in the security of our election systems. Neither is acceptable.

The draft requirements for the VVSG 2.0 developed by the Technical Guidelines Development Committee (TGDC), and affirmed by the Standards Board and Board of Advisors, in compliance with requirements in the Help America Vote Act of 2002, do not permit the inclusion of devices capable of connecting voting systems to networks wirelessly.

Principle 14 of the draft VVSG 2.0 delivered to the EAC by the TGDC protects system integrity through specific guidelines, under principle 14, Guideline 14.2 clearly requires that:

14.2 – The voting system limits its attack surface by avoiding unnecessary code, data paths, connectivity, and physical ports, and by using other technical controls.

This is further elucidated in guideline 14.2.D which specifies that voting systems *must not include the capability to establish wireless connections.*

EAC removed recommended prohibitions for wireless networking configuration

- **Permits networking capability** ⟷ ***"Grave mistake as it would significantly increase the potential for remote cyber-attacks on voting systems"***
- **Known remote system access methods-**
  - **Unintentional misconfiguration**
  - **A software update**
  - **Technical error**

Ohio law should require voting system equipment certification standards with greater rigor than EAC published VVSG 2.0

Ohio Law Disconnect with Federal Law

Current approved voting system certification standard is VVSG 2.0 (2021)

	Certified Votings Systems	Election Assistance Commission Test & Certification Program		
2	Voting System (Name/Version)	Manufacturer	Testing Standard	Date Certified
3	Assure 1.2	Premier Election Solutions, Inc. (formerly Diebold Election Systems, Inc.)	VSS 2002	8/6/2009
4	ClearVote 2.1	Clear Ballot Group, Inc.	VVSG 1.0 (2005)	10/21/2019
5	ClearVote 2.2	Clear Ballot Group, Inc.	VVSG 1.0 (2005)	12/23/2021
6	ClearVote 2.3	Clear Ballot Group, Inc.	VVSG 1.0 (2005)	10/31/2022
7	Democracy Suite 4.14 Modification	Dominion Voting Systems Corp	VVSG 1.0 (2005)	7/18/2013
8	Democracy Suite 4.14-D Modification	Dominion Voting Systems Corp	VVSG 1.0 (2005)	11/25/2014
9	Democracy Suite 4.14-E Modification	Dominion Voting Systems Corp	VVSG 1.0 (2005)	7/2/2015
10	Democracy Suite 5.0	Dominion Voting Systems Corp	VVSG 1.0 (2005)	2/8/2017
11	Democracy Suite 5.0-A	Dominion Voting Systems Corp	VVSG 1.0 (2005)	8/14/2017
12	Democracy Suite 5.17	Dominion Voting Systems Corp	VVSG 1.0 (2005)	3/16/2023
13	Democracy Suite 5.5	Dominion Voting Systems Corp	VVSG 1.0 (2005)	9/14/2018
14	Democracy Suite 5.5-A (Modification)	Dominion Voting Systems Corp	VVSG 1.0 (2005)	1/19/2019
15	Democracy Suite 5.5-C	Dominion Voting Systems Corp	VVSG 1.0 (2005)	7/9/2020
16	Democracy Suite 5.5-D	Dominion Voting Systems Corp	VVSG 1.0 (2005)	6/8/2022

WHY NOT USE 2.0?

Sec. 3506.05 "Certification of Voting & Tabulating Equipment"

(H)(4)(a) "Any voting machine, marking device, or automatic tabulating equipment used in this state shall meet, ***as a condition of continued certification and use, the voting system standards adopted by the federal election commission in 2002 OR voluntary voting system guidelines most recently adopted by the election assistance commission."***

OH Law Disconnect

National Association of State Election Directors:

"Voting systems certified to the [old standard] will remain federally certified after November 15th 2023, and jurisdictions can continue using & purchasing those systems consistent with state laws and regulations." –Mar 2023

Source: U.S. Election Assistance Commission (eac.gov)-10 Aug 23

Transfer of voting system standards authority from FEC to the EAC under 2002 HAVA, supersedes Ohio's 2016 law citing FEC as system certification entity

OH-REP-24-1295, 1296-A-000082

Current Ohio Election Security Measures – The Gap

- In 2019, OH initiated a ***network security monitoring service*** w/DHS Center for Internet Security

  Special intrusion detection devices known as ***"Albert Sensors"*** installed across 88 counties

  **** Intent to identify malicious or potentially harmful network activity *"based on known signatures"***

  The Gap: Inability to detect poor practices and weak system design due to lack of visibility into vendors development security practices

  The Approach: Evaluate ***system security design upfront to discover system threats, vulnerabilities, malware and malicious software*** during *system production and build prior to customer delivery*

  *****No vendor directed by State to comply with security build practices as condition of certification***

Full cybersecurity unattainable without vendor security development practices disclosure

Cybersecurity Functions Framework

	Status of Voting System	Core Functions
MISSING	• *In-Development*	• *Identify*
		• *Protect*
CURRENT	• Delivered	• Detect
	• Fielded	• Respond
		• Recovery

Security review of vendor practices

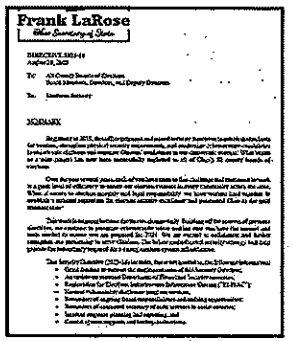
1 ***State Level Partnership (Certification)***

Collaboration

Ohio Cyber Reserve
+
Board of Voting Machine Examiners

2 Federal Level Partnership

End point security services (ESS)


Frank LaRose
Ohio Secretary of State

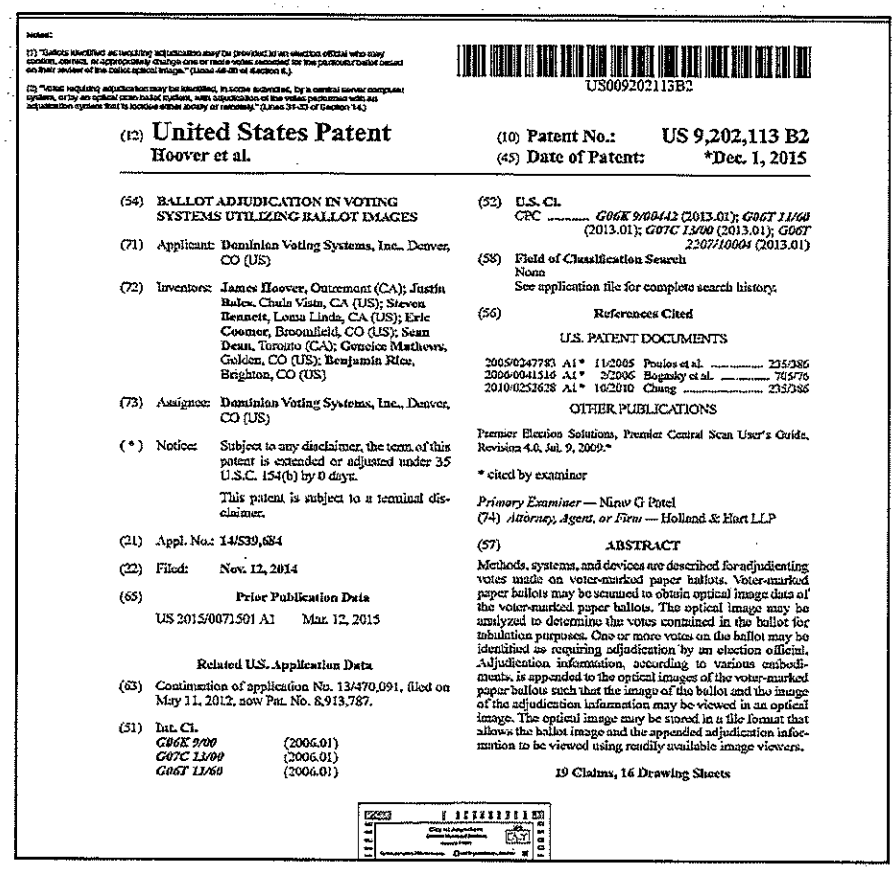
SoS Directive 2023-16 (Aug 28th 2023)

Collaboration

Ohio SoS
+
Dept of Homeland Security/
Center for Internet Security
*Crowdstrike (Vendor)

Ohio solves for *Detection, Responding & Recovering* but NOT
The earlier security flaws are remediated in development, the less effort and cost

Wireless Network Connectivity Configuration – Patent Example



US009202113B2

(12) **United States Patent**
Hoover et al.

(10) **Patent No.: US 9,202,113 B2**
(45) **Date of Patent: *Dec. 1, 2015**

(54) **BALLOT ADJUDICATION IN VOTING SYSTEMS UTILIZING BALLOT IMAGES**

(71) Applicant: Dominion Voting Systems, Inc., Denver, CO (US)

(72) Inventors: James Hoover, Outremont (CA); Justin Bales, Chula Vista, CA (US); Steven Bennett, Loma Linda, CA (US); Eric Coomer, Broomfield, CO (US); Sean Dean, Toronto (CA); Genevice Mathews, Golden, CO (US); Benjamin Rice, Brighton, CO (US)

(73) Assignee: Dominion Voting Systems, Inc., Denver, CO (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: 14/539,684

(22) Filed: Nov. 12, 2014

(65) **Prior Publication Data**

US 2015/0071501 A1 Mar. 12, 2015

Related U.S. Application Data

(63) Continuation of application No. 13/470,091, filed on May 11, 2012, now Pat. No. 8,913,787.

(51) Int. Cl.
G06K 9/00 (2006.01)
G07C 13/00 (2006.01)
G06T 11/60 (2006.01)

(52) U.S. Cl.
CPC *G06K 9/00442* (2013.01); *G06T 11/60* (2013.01); *G07C 13/00* (2013.01); *G06T 2207/10004* (2013.01)

(58) Field of Classification Search
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2005/0247783 A1* 11/2005 Poulos et al. 235/386
2006/0041516 A1* 2/2006 Bogosky et al. 705/75
2010/0252628 A1* 10/2010 Chang 235/386

OTHER PUBLICATIONS

Premier Election Solutions, Premier Central Scan User's Guide, Revision 4.0, Jul. 9, 2009.*

* cited by examiner

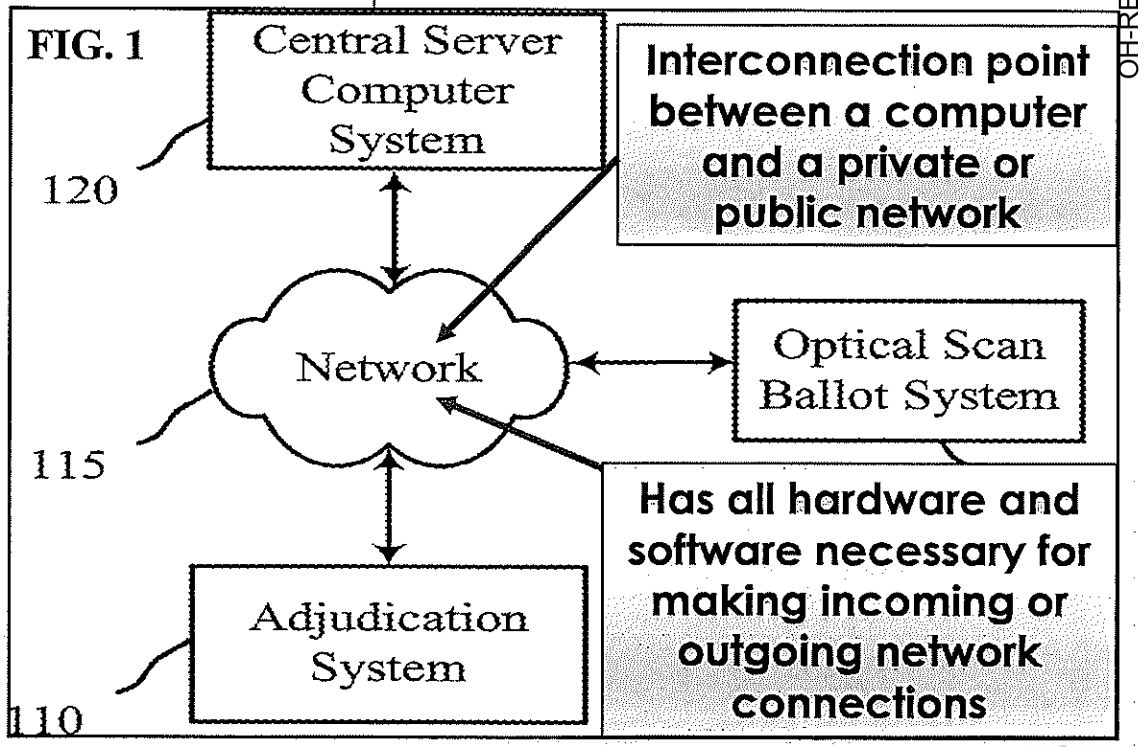
Primary Examiner — Nirav G Patel
(74) *Attorney, Agent, or Firm* — Holland & Hart LLP

(57) **ABSTRACT**

Methods, systems, and devices are described for adjudicating votes made on voter-marked paper ballots. Voter-marked paper ballots may be scanned to obtain optical image data of the voter-marked paper ballots. The optical image may be analyzed to determine the votes contained in the ballot for tabulation purposes. One or more votes on the ballot may be identified as requiring adjudication by an election official. Adjudication information, according to various embodiments, is appended to the optical images of the voter-marked paper ballots such that the image of the ballot and the image of the adjudication information may be viewed in an optical image. The optical image may be stored in a file format that allows the ballot image and the appended adjudication information to be viewed using readily available image viewers.

19 Claims, 16 Drawing Sheets

"May include multiple computers located locally and/*or remotely*"



While user can disable the wireless network from within the application, the user cannot disable the network interface on the device, the device's network card remains online and will send and receive

Current Law vs. Standard (Election Systems)

1 Ohio Law (2006) ⟷ Ohio SoS Standard (2021) **2**

OHIO LAWS & ADMINISTRATIVE RULES
LEGISLATIVE SERVICE COMMISSION

HOME LAWS ABOUT CONTACT RELATED SITES GO TO

The Legislative Service Commission staff updates the Revised Code on an ongoing basis, as it completes its act review of during some times of the year, depending on the volume of enacted legislation.

Section 3506.23 | Voting machines not to be connected to internet.
Ohio Revised Code / Title 35 Elections / Chapter 3506 Voting And Tabulating Equipment

Previous Next

Effective: May 2, 2006 Latest Legislation: House Bill 5 - 126th General Assembly PDF: Download Authenticated PDF

A voting machine shall not be connected to the internet.

Ohio's current laws leave voting systems unprotected from cyber attacks

Ohio Voting System Requirements Matrix
Revised June 15, 2021

3. **Equipment has been certified by an independent testing authority as meeting or exceeding the minimum requirements of the U.S. Election Assistance Commission voting system standards (OAC 111:3-9-08(C)(15)).**

Acceptable ☐ Not Acceptable ☐

Covered in EAC Test Report/VSTL Test Materials? Yes ☐ No ☐ N/A ☐
Additional Information Concerning Testing Information:

Comments:

4. **A voting machine shall not be connected to the Internet (R.C. 3506.23). A voting system or voting machine is prohibited from containing any wireless communication hardware or software components.**

Acceptable ☐ Not Acceptable ☐

Covered in EAC Test Report/VSTL Test Materials? Yes ☐ No ☐ N/A ☐
Additional Information Concerning Testing Information:

Comments:

Update Ohio law with Wireless Communication Restrictions: "Voting systems must not be capable of establishing wireless connections"

4

Make Current SoS Rule OH Law: "A voting system or voting machine is prohibited from containing any wireless communication hardware or software components"

3

5

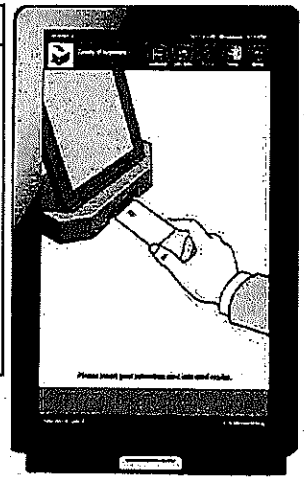
As condition of certification, enforce security development practices & previous build activities disclosure requirements upon election system vendor-developers

Threats to Auditability – Ohio Use Case (DREs)

- ***Touchscreen Direct Record Electronic (DRE) Voting Equipment***
  - ***Diminished verifiability creates auditing and federal compliance issue***
  - ***Deprive voters of the right to know-***
    - *"Election results are determined from Ballot QR codes, which malware can modify, yet voters cannot check that the QR codes match their intent, nor does the state compare them to the human-readable ballot text" – Halderman Report (2023)*

VOTING EQUIPMENT	COUNTY
Dominion Image Cast X (ADA) (direct recording electronic (DRE) with voter-verified paper audit trail (VVPAT))	Adams
	Butler
	Fairfield
	Greene
	Hancock
	Hardin
	Perry
	Richland
	Scioto
	Stark
	Wayne
	Wood

Ohio counties using DREs Voting Machines



Key Insights: Dominion ImageCast X Voting (DRE) Equipment

- *Scanners ignore the ballot text and count the votes encoded in the QR code not voter "Selection Summaries"*
- *QR code produces the cast vote record not the VVPAT, prohibiting HAVA Title III required auditability*
- Security design does not protect against duplicated QR codes or malware running on Ballot Marking Device (BMD)

Voter intent read from a QR code does NOT meet HAVA Title III 'Voting System Standards Manual Audit Capacity' requirement for auditable paper record

Computerized Voting Systems - Security Vulnerabilities

- ***Dominion ImageCast X (ICX) Ballot Marking Device (BMD)***
  - ***Principal Findings*** – **"ICX suffers from critical vulnerabilities" Altered both QR codes and human text**

Most Serious Vulnerabilities– (Halderman Report 2023)

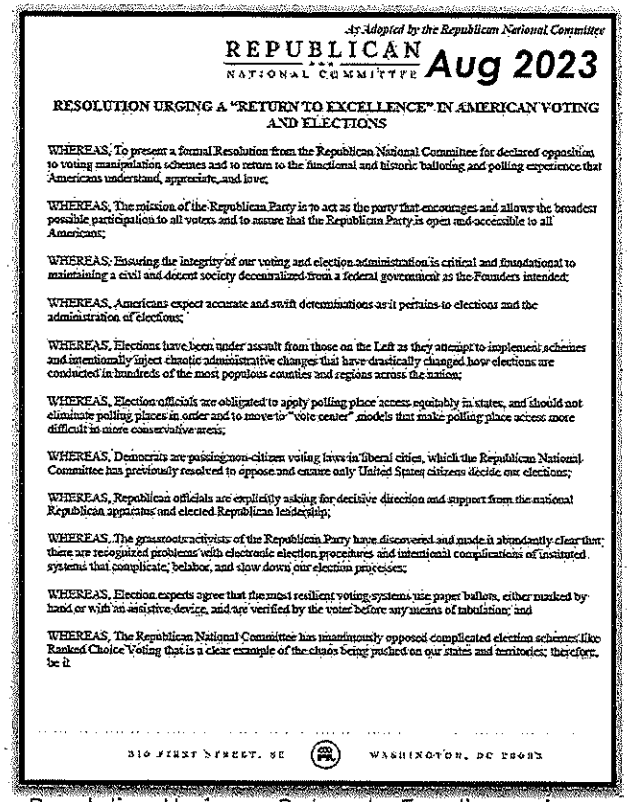
- Attackers ***altered QR codes on printed ballots*** to modify voters' selections
- ***Software updates*** lead to potential access/***malware install in polling place***
- ***Forged & manipulated smart cards*** used unlock any ICX and install malware
- ***Altered election definition*** **files** via arbitrary code, ***can exploit all machines in the county***
- ***Access to scanner's memory card violate ballot secrecy*** by dishonest election worker
- Alteration of audit logs through access of ***unnecessary Android applications***
- ***Obtained county-wide keys via access to single ICX and Poll Worker Card & Pin,***
  - *All scanners & BMDs share same set of cryptographic keys for authentication*

Key Takeaway: ***BMDs and DREs in use in Ohio "developed without sufficient attention to security during design, software engineering and test…small mistake can lead to complete exploitation"***

BMDs and DREs are "not sufficiently secured to withstand vote-altering attacks"

National Resolution – Republican National Committee (RNC)

- "The grassroots activists…discovered and made abundantly clear ***there are recognized problems with electronic election procedures"***
- **"Election experts agree that <u>the most resilient voting systems use paper ballots</u>, …verified by the voter before means of tabulation"**
- "**<u>RNC boldly opposes means of voting</u>** that do not have proper safeguards…and are **<u>exclusively electronic…</u>*calls on every county and state in the nation to use default ballot systems, which are fully auditable, namely hand-marked, voter-verified paper ballots***
- **"RNC supports** the rights of **counties and states that** are willing and able to competently and efficiently **<u>implement voting procedures that do no require the use of machines</u>** and those **that implement hand counting procedures <u>that are fully auditable</u>"**
- **"RNC <u>call on state legislatures</u>, county, and municipal codes and rules <u>that allow for full transparent hand-counting procedures</u> that are planned, timely and fully observable"**
- "The **RNC calls on all Republican officeholders to <u>defend…assigned precinct, ward and localized polling places for means of balloting and tabulating paper ballots by geographic unit</u>"**



As Adopted by the Republican National Committee

REPUBLICAN NATIONAL COMMITTEE **Aug 2023**

RESOLUTION URGING A "RETURN TO EXCELLENCE" IN AMERICAN VOTING AND ELECTIONS

WHEREAS, To present a formal Resolution from the Republican National Committee for declared opposition to voting manipulation schemes and to return to the functional and historic balloting and polling experience that Americans understand, appreciate, and love;

WHEREAS, The mission of the Republican Party is to act as the party that encourages and allows the broadest possible participation to all voters and to assure that the Republican Party is open and accessible to all Americans;

WHEREAS, Ensuring the integrity of our voting and election administration is critical and foundational to maintaining a civil and decent society decentralized from a federal government as the Founders intended;

WHEREAS, Americans expect accurate and swift determinations as it pertains to elections and the administration of elections;

WHEREAS, Elections have been under assault from those on the Left as they attempt to implement schemes and intentionally inject chaotic administrative changes that have drastically changed how elections are conducted in hundreds of the most populous counties and regions across the nation;

WHEREAS, Election officials are obligated to apply polling place access equitably in states, and should not eliminate polling places in order and to move to "vote center" models that make polling place access more difficult in more conservative areas;

WHEREAS, Democrats are passing non-citizen voting laws in liberal cities, which the Republican National Committee has previously resolved to oppose and ensure only United States citizens decide our elections;

WHEREAS, Republican officials are explicitly asking for decisive direction and support from the national Republican apparatus and elected Republican leadership;

WHEREAS, The grassroots activists of the Republican Party have discovered and made it abundantly clear that; there are recognized problems with electronic election procedures and intentional complications of instituted systems that complicate, belabor, and slow down our election processes;

WHEREAS, Election experts agree that the most resilient voting systems use paper ballots, either marked by hand or with an assistive device, and are verified by the voter before any means of tabulation; and

WHEREAS, The Republican National Committee has unanimously opposed complicated election schemes like Ranked Choice Voting that is a clear example of the chaos being pushed on our states and territories; therefore, be it

310 FIRST STREET, SE WASHINGTON, DC 20003

Resolution-Urging-a-Return-to-Excellence-in-American-Voting-and-Elections.pdf (gop.com)

Unanimous resolution calling State legislatures to <u>pass laws</u> allowing full transparent hand-counting procedures at precinct and local polling places for means of balloting and tabulation

Election Infrastructure – Cost Benefit Analysis

Butler County, Ohio ~ 1x Purchase Agreement $6.1M

- $6.1M X 88 Counties = ~ +$536M for Ohio Vendor Contracts

EXHIBIT A

TO THE VOTING SYSTEM AND SERVICES AGREEMENT
BY AND BETWEEN DOMINION VOTING SYSTEMS, INC.
AND THE COUNTY OF BUTLER, OHIO

PRICING SUMMARY AND DELIVERABLES DESCRIPTION

1. Pricing Summary - Prices of equipment, technical facilities, software, and other related services for voting, vote counting, and result processing. All pricing in U.S. Dollars.

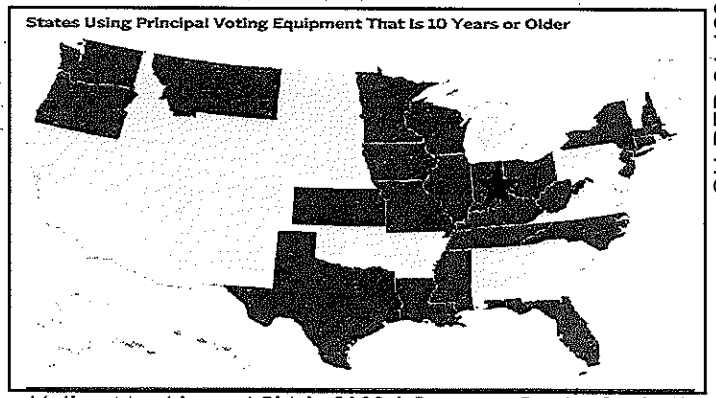
Table A: State-Funded Items pursuant to Exhibit C

DESCRIPTION	QTY	UNIT PRICE	EXTENSION PRICE
Central Scanning Solution: Absentee / Vote By Mail Hardware			
ImageCast Central Kit: Canon DR-G1130 high speed document scanner includes: ImageCast Central Software, Dell OptiPlex All-in-One, iButton programmer and key, cables	3	$ 25,000.00	$ 75,000.00
Sub-Total:			$75,000.00
In-Person Voting Solution: Polling Location Hardware			
ImageCast X BMD w/VVPAT (21 inch) Kit includes: ICX Firmware, Tablet, 5 voter activation cards, VVPAT, cables, power cord	1,500	$ 3,500.00	$5,250,000.00
ATI Accessible Voting Kit for ICX USB	100	$ 375.00	$37,500.00
ImageCast X Voting Leg Stand	1,500	$250.00	$375,000.00
MBP System includes OKI Data C931E printer, laptop, cables	3	$11,560.00	$34,680.00
ICX Pollworker Smartcard	900	$ 8.00	$7,200.00
ICX Technician Smartcard	150	$ 8.00	$1,200.00
Dual Bay Battery Charger	50	$ 165.00	$8,250.00
8GB USB Flash Drive	1,500	$17.00	$25,500.00
Sub-Total:			$5,739,330.00
Election Management Hardware			
Democracy Suite EMS Express Server - up to 7 clients	1	$ 17,000.00	$ 17,000.00
EMS Client Workstation Configuration Kit	1	$ 2,500.00	$ 2,500.00
EMS Report Printer	2	$ 250.00	$ 500.00
Adjudication workstation	2	$1,500.00	$3,000.00
Smart Card Reader/Writer	5	$22.00	$110.00
Sub-Total:			$23,910.00
Software License Fee			
Democracy Suite (EMS) Application	1	$ 170,000.00	$ 170,000.00
Adjudication Software	1	$35,000.00	$35,000.00
Mobile Ballot Printing	1	$6,500.00	$6,500.00
			$211,500.00
Implementation Services	Days		
Voting System Deployment (e.g., software, installation & configuration, acceptance testing, etc.)	70	$ 2,000.00	$140,000.00

Dominion Voting Systems Inc.
Exhibit A – 5.10.2019

Butler County Purchase Agreement
Page 1 of 7

What is the <u>cost-benefit analysis</u> of an exclusively electronic voting system vs. blend of hand-marked paper ballot counting?



Voting Machines at Risk in 2022 | Brennan Center for Justice

Knowing computerized voting systems have known technical design security flaws and remote system threat access points enabled by activated wireless configuration that enable cyber exploitation and attack vulnerabilities....

How do we secure tens of millions of dollars worth of computerized voting system investment and restore public confidence without introducing real vendor accountability or oversight transparency of product development?

Reduce election system risk by requiring vendor-developers disclose system development security practices, foreign ownership and attest to software supply chain integrity

Ohio County BOE Engagement – Cost Benefit Analysis

17 August 2023

Greene County Republican Central Committee, Cost Benefit SubCommittee

Subject: Cost Benefit Analysis Committee Report **Aug 2023**

Purpose: The Cost Benefit Analysis Committee was formed to look into the costs associated with the voting machines versus paper.

Members: Katy Howard, Jo Tarka, Chip Sutton, Gary Tarka, James Johnson, Jan Basham, Frank Blackstone, Carolyn Uecker, Nancy Maxwell, and Anita Swan, Chair

We contacted the Director of the Greene County Board of Elections, Alisha Beeler Lambert, who gave us the background regarding the voting machines we currently use in Greene County. The Dominion machines were procured in 2018 and put into service in 2019. They have a life expectancy of approximately 7-9 years. In addition to storage, testing and transportation expenses, there are annual licensing and maintenance fees associated with the voting machines. Greene County's population is approximately 168K.

We met with the Director of Clark County Board of Elections, Jason Baker. Clark Country uses only paper for their elections. Mr Baker was very gracious with his time and showed us the Clark Country voting process, the storage facilities and the tabulating process. Clark County's population is approximately 136K.

We also met with the Director of Montgomery County Board of Elections, Jeff Rezabek. Mr Rezabek was also very gracious with his time. Montgomery County uses both voting machines (ES&S) and paper during their elections, the voter selects which method to use. Mr Rezabek showed us the voting processes (paper and voting machines), storage and tabulating process. Montgomery Country recently conducted a cost comparison between using only paper or only machines for elections. The difference between the all paper versus all machines was significant (approximately $7.5M cost avoidance over a 10 year period). Montgomery County is recommending they move to all paper voting. Montgomery County's population is approximately 537K.

Note: If voting by paper ballot this requires a scanner/tabulator to "read" the ballot and tabulate the votes. These are not connected to the internet.

Conclusion: Both Montgomery County and Clark County have proven that the paper voting process is feasible and efficient. While the Montgomery County machines are different than the voting machines, we use here in Greene County we fully expect that there will be a large cost avoidance if Greene County moves to all paper voting rather than repracuring and/or replacing/refurbishing our voting machines when the time comes. We recommend the Director of Greene County Board of Elections conduct a cost comparison between all paper voting versus machine voting and if, as expected, there is a significant cost avoidance, that Greene County move to all paper voting.

Respectfully,

Anita Swan, Chair, Cost Benefit Analysis Committee

- ***Engagement with Clark, Greene and Montgomery County BOEs***
  - Voting machine life expectancy 7-9 years (2019-2028)
  - Montgomery County cost benefit analysis between all paper and all machines indicated $7.5M cost savings over 10 years
    - "Montgomery County is recommending they move to all paper voting"

Recommendation: "We recommend the Director of Greene County BOE conduct a cost-comparison between all paper voting versus machine voting and if, as expected, there is a significant cost avoidance, that Green County move to all paper voting"

"Both Montgomery and Clark County have proven that the paper voting process is feasible and efficient"

Greene County - Opposing Resolution on DREs

Objectivity Deficit – Conflict of interest

- "Voting Machine contractor employees are involved in the audit and certification of their own machines before, during and after the election process"

Non-transparency – Questionable integrity of election process

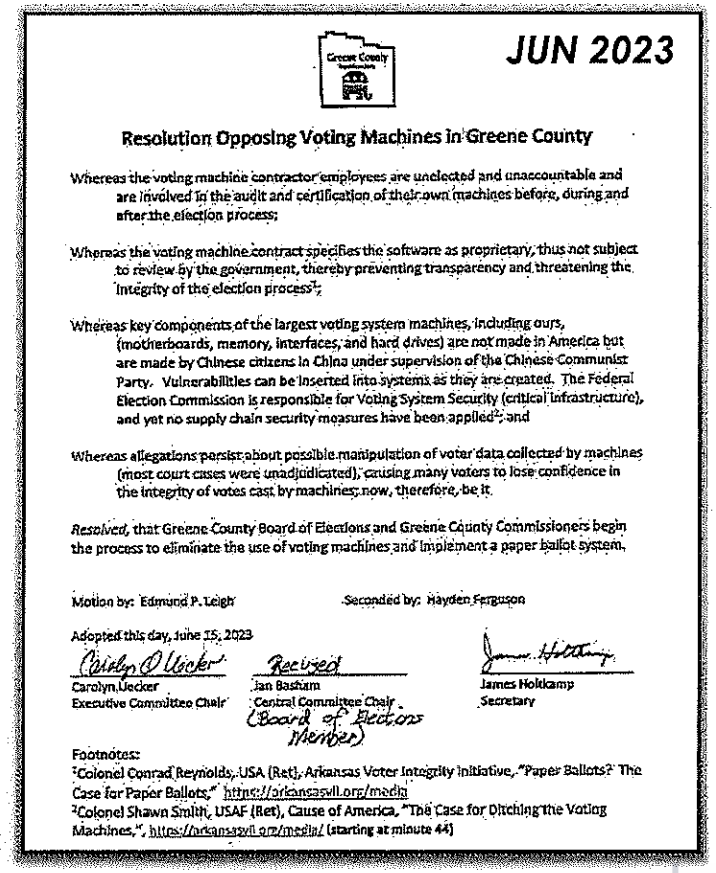
- "Voting machine contract specifies the software as proprietary, not subject to review by the government"

Supply chain integrity – Unaccounted and non-reviewable

- "Key components of voting system machines, (motherboards, memory, interfaces, and hard drives) are not made in America but made by Chinese citizens"
- "EAC is responsible for Voting system security and yet no supply chain security measures have been applied."

Public confidence in computerized voting systems decreasing

- "Allegations persist about possible manipulation of voter data (most court cases were unadjudicated), causing voters to lose confidence in integrity of votes cast by machines"



JUN 2023

Resolution Opposing Voting Machines in Greene County

Whereas the voting machine contractor employees are unelected and unaccountable and are involved in the audit and certification of their own machines before, during and after the election process;

Whereas the voting machine contract specifies the software as proprietary, thus not subject to review by the government, thereby preventing transparency and threatening the integrity of the election process[1];

Whereas key components of the largest voting system machines, including ours, (motherboards, memory, interfaces, and hard drives) are not made in America but are made by Chinese citizens in China under supervision of the Chinese Communist Party. Vulnerabilities can be inserted into systems as they are created. The Federal Election Commission is responsible for Voting System Security (critical infrastructure), and yet no supply chain security measures have been applied[2]; and

Whereas allegations persist about possible manipulation of voter data collected by machines (most court cases were unadjudicated), causing many voters to lose confidence in the integrity of votes cast by machines; now, therefore, be it

Resolved, that Greene County Board of Elections and Greene County Commissioners begin the process to eliminate the use of voting machines and implement a paper ballot system.

Motion by: Edmund P. Leigh Seconded by: Hayden Ferguson

Adopted this day, June 15, 2023

Carolyn Uecker — Executive Committee Chair

Received — Ian Basham, Central Committee Chair (Board of Elections Member)

James Holtkamp — Secretary

Footnotes:
[1]Colonel Conrad Reynolds, USA (Ret), Arkansas Voter Integrity Initiative, "Paper Ballots? The Case for Paper Ballots," https://arkansasvii.org/media
[2]Colonel Shawn Smith, USAF (Ret), Cause of America, "The Case for Ditching the Voting Machines,", https://arkansasvii.org/media/ (starting at minute 44)

All voting systems face cybersecurity risks, not all voting systems are equally vulnerable

Opt-Out Clause: Criteria & Alternatives

Establish criteria to determine primary method for casting, recording & tabulating ballots in the event a voting systems fail certification standards:

Criteria Examples:

1. "All **components** have been **designed, manufactured, integrated and assembled in the U.S.** from trusted suppliers, using trusted processes accredited by the Defense Microelectronic Activity as prescribed by Dept of Defense
2. The **source code** used in any computerized voting machine for federal elections is **made available to the public or designated state directed cyber security review entity**
3. The **ballot images and system log files from each tabulator** are recorded on a secure write-once, read-many media with clear chain of custody and **posted on the Secretary of State's website** free of charge to the public within 24-72 hours after the close of polls

- Defense Microelectronics Activity - AccreditedSuppliers.pdf (osd.mil)

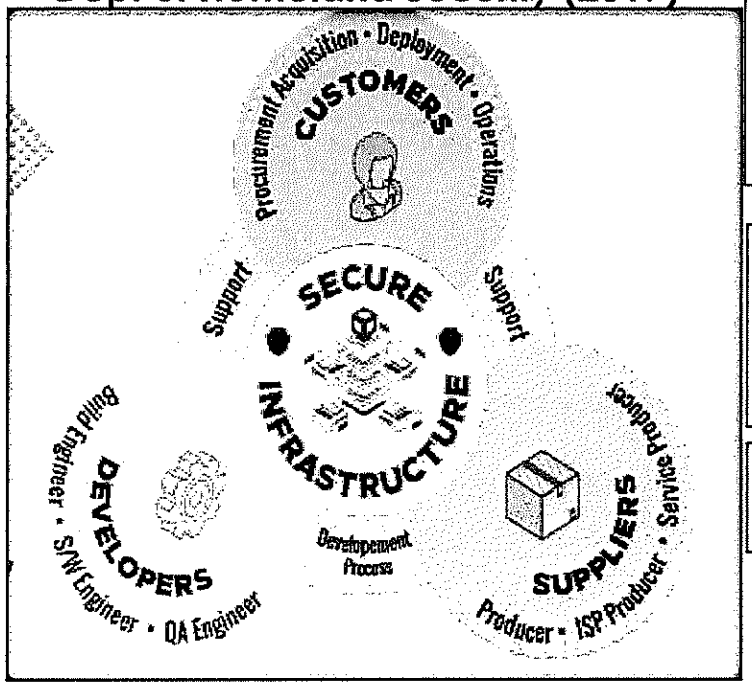
What will counties do if voting systems are de-certified?

Incorporate county machine-use opt-out provision into Sec 3506.05 in event of voting system de-certification?

Initiate a legislative study and/or county pilot project to study feasibility of primary hand-marked paper ballot counting at the precinct level

Ohio Voting System Certification – The Solution

Elections are
"National Critical Infrastructure"
-Dept of Homeland Security (2017)

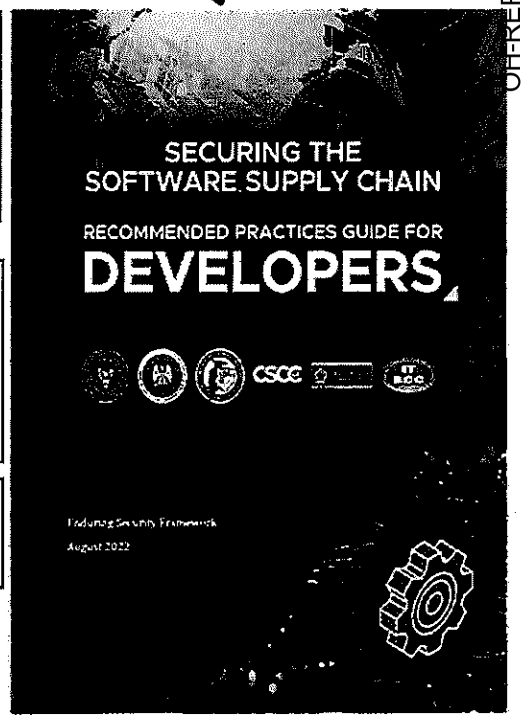


Codify following provisions into law:

1. ***Codify SoS system requirement rule*** prohibiting wireless hardware/software component in voting machines

2. ***Vendors adhere to federal security development practices*** *and disclose voting system development practices* ***as condition of certification***

3. ***Introduce in-state 3rd party Cyber Security Reviews***



Empower OHIO CYBER RESERVE to lead certification security reviews in partnership with SOS as a pre-requisite to election voting system selection and County BOE procurement

Revised Ohio Law - Security Certification Provisions

Vendor-Developer Provisions:

- **Adopt *software supply chain integrity security development best practices****
- **Require *security development build practices disclosure***
- ***Include background checks and security measures for personnel****
- ***Disclose vendor & subcontractor foreign ownership****
- ***Requirement and processes for reporting cyber incidents****
- ***Require Software Bill of Materials (SBOM)***
- **Accept recurring *State-directed 3rd party regular system build audits,*** penetration testing and physical site inspections
- ***Accept publication of system security review team findings on SoS website*** for public transparency

Brennan Center for Justice, "A Framework for Election Vendor Oversight: Safeguarding America's Election Systems (2019)

Update Section 3506.10 | Requirements for approval or certification of voting machines
Effective: May 7, 2004

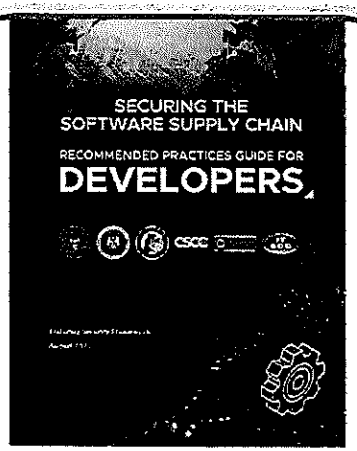
Vendor Cyber Certifiability – Requirement Standards

Appendix D: Artifacts and Checklists

Producible Items

1. High-level Secure Development Lifecycle Process Document
2. Product Readiness Checklist
3. Product Support/Response Plan
4. Software Bill of Material (SBOM)
5. Architecture/Design Documents
6. Developer Training Certificates/Training Completion Statistics/data
7. Threat Model Results Document
8. High-level Software Security Test Plan and Results
9. Automatic and Manual Dynamic and Static Security/Vulnerability Reports (Security Scanning Results) Reports
10. Open Source Review Process Document and Allowed List
11. Build Log
12. Secure Development Build Configurations Listing
13. Third-Party Software Tool-Chains List

1



2

OHIO CYBER RESERVE
OhCR

Decision Point

Frank LaRose
Ohio Secretary of State

4

3

OH BOARD of VOTING SYSTEMS EXAMINERS

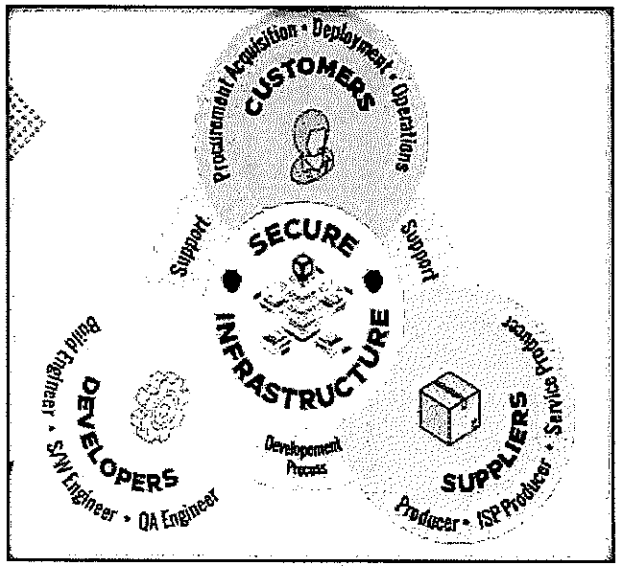
Ohio Cyber Reserve will perform cyber security verification of vendor-developer systems and submit report to OH SoS for Certification determination and public disclosure disclosure

Summary

Challenges

- ***No federal certification standards for most voting systems*** products and services
- Election systems ***continue to certify to obsolete 2005 security standards*** through 2023
- ***No election vendor oversight*** for software supply chain integrity & security development practices
- ***BMD and DRE voting machines not secured to withstand "vote altering attacks,"*** known threats can **falsify** voter intent & fail ***auditability under HAVA Title III via QR code***

Recap



Questions?

Solutions

- ***Codify SoS system requirement rule prohibiting wireless hardware/software components*** in voting machines
- **Vendors shall adhere to federal security development practices**, disclose software byproducts (i.e. artifacts) & agree to 3rd party security review **as condition of certification**
- **Direct Ohio Cyber Reserve to conduct security analysis review** of election vendor systems
- **Sunset DRE Voting Machines,** insufficiently secured, non-auditable
- **Specify County machine opt-clause for system de-certification** & hand-marked paper ballot counting pilot studies

Securing Ohio's Voter Registration Systems

A Legislative Approach and Cyber Security Perspective

Ohio Election Study Collaborative

Presenter: Marcell Strbich

October 30th 2023

The views expressed are those of the individual only and not those of the U.S. Air Force or Dept of Defense

Overview

- Overview Blockchain Upgrade
  - Ohio Sec of State - Legislation
  - Blockchain Opportunity – Ohio 1st in the Nation Status
- Cyber Security Core Functions Framework Review
  - Cyber Security – Attack Spectrum
  - Designated Agencies Providing Registration Services
- Blockchain Vs. Traditional Database Comparability
  - Voter Registration Database – Functional Design Limitations
  - Blockchain Digital Ledger Database – Features Explained
  - Blockchain Use Case - Overview
- Blockchain Digital Ledger – Deployment Configurations
  - Blockchain Use Case – Centralized with Operational Data
  - Blockchain Use Case – Centralized with Non-Operational Data
  - Security Model – Authentication and Authorization
- Ohio Voting System Certification – The Solution
  - Summary Recap

Overview - Blockchain Upgrade (Modernizing Databases)

Databases are software systems that store large collections of data for fast lookup, correlation, reporting, and retrieval by software application

Establishing trust around the integrity of data stored in database systems has been a longstanding problem for all organizations that manage sensitive data

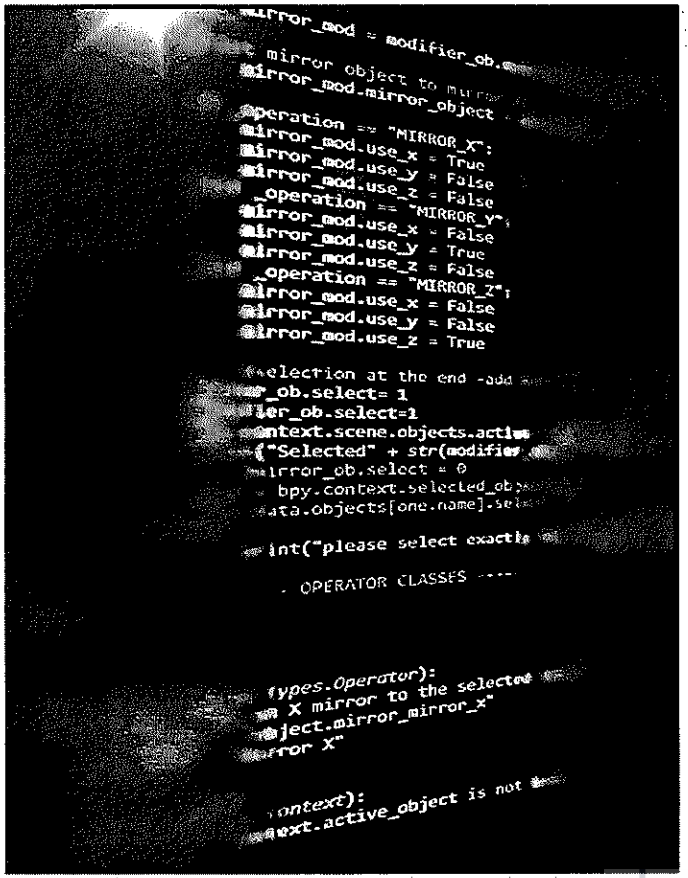
Voter Registration Database data is vulnerable

Existing database lacks tamper resistance/ tamper evidence capabilities

Existing database lacks group validation and consensus mechanism to reduce risk of malicious alteration

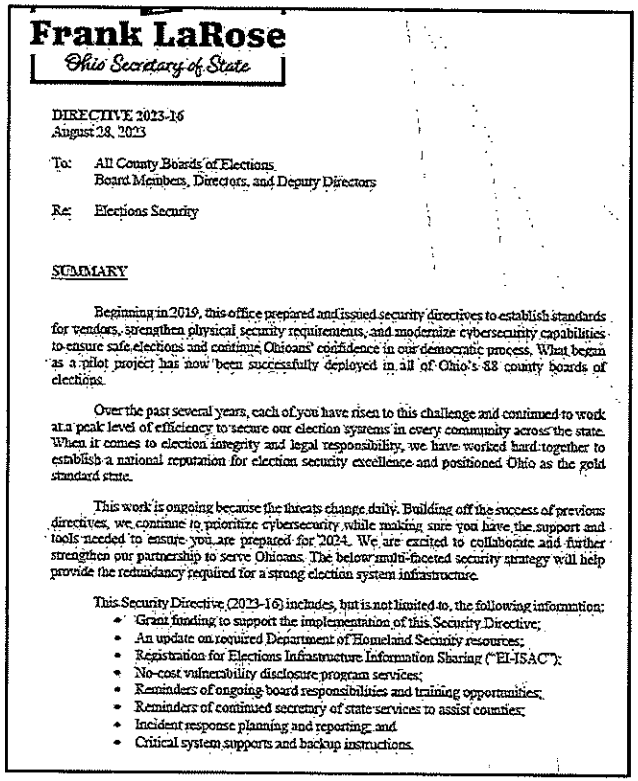
Existing database does not preserve data value in maintained co-located history table

Existing data values and transactions do not utilize cryptographic security controls or multi-factor authentication for verification



Transformative Opportunity to Secure Voter Roll Integrity and establish System Wide Transparent Auditability for Proof of Malicious Data Alteration

Ohio Sec of State – Legislation



Frank LaRose
Ohio Secretary of State

DIRECTIVE 2023-16
August 28, 2023

To: All County Boards of Elections
Board Members, Directors, and Deputy Directors

Re: Elections Security

SUMMARY

Beginning in 2019, this office prepared and issued security directives to establish standards for vendors, strengthen physical security requirements, and modernize cybersecurity capabilities to ensure safe elections and continue Ohioans' confidence in our democratic process. What began as a pilot project has now been successfully deployed in all of Ohio's 88 county boards of elections.

Over the past several years, each of you have risen to this challenge and continued to work at a peak level of efficiency to secure our election systems in every community across the state. When it comes to election integrity and legal responsibility, we have worked hard together to establish a national reputation for election security excellence and positioned Ohio as the gold standard state.

This work is ongoing because the threats change daily. Building off the success of previous directives, we continue to prioritize cybersecurity while making sure you have the support and tools needed to ensure you are prepared for 2024. We are excited to collaborate and further strengthen our partnership to serve Ohioans. The below multi-faceted security strategy will help provide the redundancy required for a strong election system infrastructure.

This Security Directive (2023-16) includes, but is not limited to, the following information:

- Grant funding to support the implementation of this Security Directive;
- An update on required Department of Homeland Security resources;
- Registration for Elections Infrastructure Information Sharing ("EI-ISAC");
- No-cost vulnerability disclosure program services;
- Reminders of ongoing board responsibilities and training opportunities;
- Reminders of continued secretary of state services to assist counties;
- Incident response planning and reporting; and
- Critical system supports and backup instructions.

SoS Directive 2023-16 (Aug 28th 2023)

"We have worked hard together to establish a national reputation for election security excellence and positioned Ohio as the gold standard state"
–OH Sec of State Frank LaRose

Legislative Achievements [2019-2023]

- S.B. 52 Creation of the Ohio Cyber Reserve Force
- H.B. 458 Voter Identification
- S.B. 51 Creation of Election Integrity Division
- S.B. 71 Data Analysis and Transparency Archives Act (DATA Act)

Next:

- Modernize Voter Registration System Certification Standards
  - Adopt Blockchain Digital Ledger Database
  - Vendor Security Development Practices Disclosure & 3rd party OH Cyber Reserve Security Assessments

Prime Opportunity to Update Voter Registration System Certification Standards Into Legislation And Enact 3rd Party Security Reviews

Blockchain Opportunity – Ohio "1st in the Nation Status"

- **1st Voter Registration DB system to adopt Blockchain digital ledger database**
  - Securely track and protect data from any attacker or high privileged user ***(i.e. lock down voter rolls)***
  - *Capable of streamlined system-wide* ***auditing to reveal attestation proof for malicious attacks***

- **1st Voter Registration DB system to feature immutability and append-only features**
  - **Tamper Resistant:** Means difficult to reversibly change and impossible to overwrite data once stored
  - **Tamper Evidence:** Means once data is stored, any changes to it are easily detected
  - Operationalizes S.B. 14 Data Analysis Transparency and Analysis Archives Act (DATA Act)

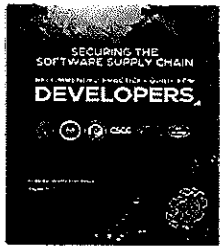
- **1st State to require election vendors adhere to and report/disclose to 3rd party independent cyber security reviewers' security development practices as condition for State-level certification**
  - Codifies into law SoS Cybersecurity Directive 2023-16 (Aug '23), "establish standards for vendors"
  - Operationalizes S.B. 52 (2019) creating Ohio Cyber Reserve to protect critical election infrastructure

Blockchain Ledger DB Adoption ensures security controls and data integrity system-wide streamlined auditing

Cybersecurity Core Functions Framework Review

	Status of Voting System	Core Functions
MISSING	• *In-Development*	• *Identify* • *Protect*
CURRENT	• Delivered • Fielded	• Detect • Respond • Recovery

Security review of vendor practices



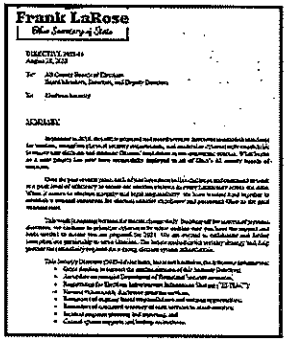
1 ***State Level Partnership (Certification)***

Collaboration

Ohio Cyber Reserve
+
Board of Voting Machine Examiners

2 Federal Level Partnership

End point security services (ESS)


Frank LaRose
Ohio Secretary of State

SoS Directive 2023-16 (Aug 28th 2023)

Collaboration

Ohio SoS
+
Dept of Homeland Security/
Center for Internet Security
*Crowdstrike (Vendor)

Ohio solves for *Detection, Responding & Recovering* but NOT
The earlier security flaws are remediated in development, the less effort and cost

Cyber Security – Attack Spectrum

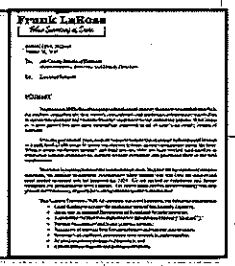
Application-Level Threats
- Input Validation Attacks
- Authentication and Authorization
- Data Exposure
- Business Logic Flaws

Software Development Life Cycle (SDLC) Threats
- Requirement Phase
- Design Phase
- Implementation Phase
- Testing Phase
- Deployment Phase
- Maintenance Phase

FEDERAL SECURITY PARTNERSHIP [DHS/OH SoS)

UPDATE STATE SECURITY LEGISLATION

Network Level Threats
- Perimeter Security
- Data Transmission
- ***Endpoint Security***
- Internal Threats


Frank LaRose
Ohio Secretary of State

SoS Directive 2023-16
(Aug 28th 2023)

Frank LaRose
Ohio Secretary of State

Contractual Aspects Implications
- Security Requirements
- Compliance and Standards
- Liabilities and Indemnities
- Data Ownership and Privacy

Evaluate *network security at the access, application and data levels* for more secure, compliant and resilient operational environment

Designated Agencies Providing Registration Services

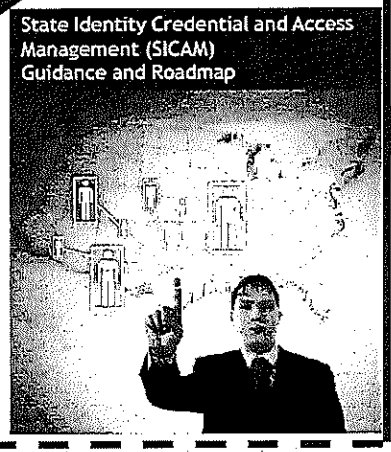
DATA ACT/2023

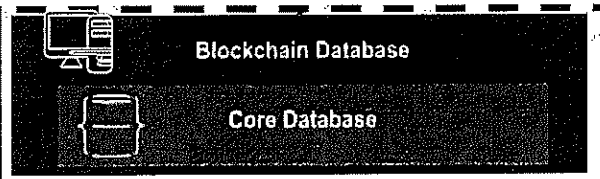
State Agencies – Database Maintenance

- Department of Health
- Bureau of Motor Vehicles
- Dept of Job and Family Services
- Dept of Medicaid
- Dept of Rehabilitation and Corrections

National Voter Registration Act (1993)

- Dept of Mental Health and Addiction Services
- Dept of Developmental Disabilities
- Opportunities for Ohioans with Disabilities
- *Ohio's four-year state-supported colleges and universities

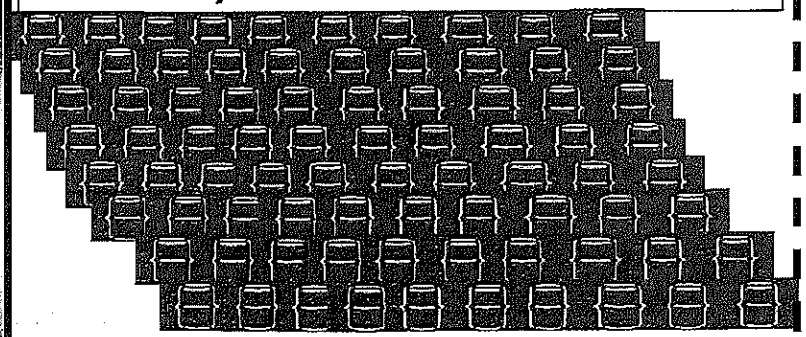




Statewide Voter Database [SOS]

County BOE Databases only interoperable with SoS Statewide Voter Registration Database, not State Agencies

88x County Board of Elections Databases



*ORC Procedural Change

Blockchain Digital Ledger Database Enables Sharing, Verifying and Trusting Data Across Multiple-Party Business Processes Participating on the Network

Blockchain vs Traditional Database Comparability

	Blockchain	Databases
Data Integrity	The blockchain structure makes it virtually impossible for someone to change the data without breaking the chain. *[Anti-Tamper Evidence]*	A malicious actor can potentially alter data if necessary measures are not taken. *[No Tamper Evidence]*
Transactions	Data can only be read or added to the blockchain. *[Immutable-Irreversible]*	Data can be created, read, updated, or deleted (CRUD operations). *[Mutable-Reversible]*
Querying Performance	The verification methods to ensure data integrity can slow down the querying and general performance of a blockchain. *[Signed-Verified]*	Databases provide blazing-fast access to the data. *[No signature verification]*
Structure	Blockchains can be fully decentralized and not rely on any central authority. *[Transparency-Redundancy]*	Databases are centrally managed, and an administrator owns and controls the data. *[No practical data controls]*

Traditional Database (Relational)

Rigid Data Structure
- Used for well structured data
- Linked by relationships
- Lookup via common value
- Fast lookup results

Inflexible Development Options
- New fields require DB rebuild if software requirements for data changes
- Time-consuming and more expensive to upgrade apps

Auditing Impractical
- History not preserved in co-located way in database
- Unable to attest to alteration

Incorporating Blockchain On Top of Traditional Databases Retains Power, Flexibility and Performance and Adds Data Integrity

Voter Registration Database – Functional Design Limitations

- **Database is accessible** to a variety of IT and database administrator staff
  - **Data vulnerable** not only to abuse of privilege, but theft of this privilege and use by adversaries
  - **Threat surface is broad**; home-based, mobile personal computers or remote access by IT staff

- ***Transactions*** within the database are ***reversible*** and ***lack tamper-proof evidence*** capabilities
  - Any actor (authorized/unauthorized) that has obtained access can freely modify content of DB
  - ***Mutable data of*** voter records ***makes data integrity verification impractical and cumbersome***

- **Audit processes are highly time-intensive costly activities**
  - ***Changed values are overwritten, history not preserved in co-located manner*** *on the database*
  - **Unable to** perform streamlined system-wide audits or **provide attestable proof of malicious alteration**
  - ***No ability to replay or reconstruct voter roll transaction history***

Voter rolls (lists) are Stored in Traditional Relational Database Management Systems, With No Practical Controls on Data Integrity

Blockchain Digital Ledger Database - Features Explained

- **Adopts Decentralization: Transparency and Redundancy**
  - **Distributed database technology** allows data to be stored across a network of computers, rather than on a single centralized server

- **Adds Security Controls: Resistant to Cyber Attacks**
  - **Provides proof of data integrity to auditors**
  - **Adopts access control verification: Multifactor Authentication (MFA):**

- **Incorporates Immutability: Key to Public Trust and Transparency**
  - Once recorded, ***transaction is extremely difficult to alter or delete*** and is ***tamper-evident to all viewers (i.e Streamlines Auditing)***
  - ***Tampering*** will ***only be possible with collusion*** among multiple parties
  - Blockchain ledger is often ***accessible to the public, allowing anyone to view the transaction history [Optional]***

Blockchains Use Digital Ledgers to Securely Store Transactional Data and Verify Integrity Through Forensics and Playback Capabilities

Blockchain Use Case - Overview

Voter Registration Database - No Federal or State certification standard

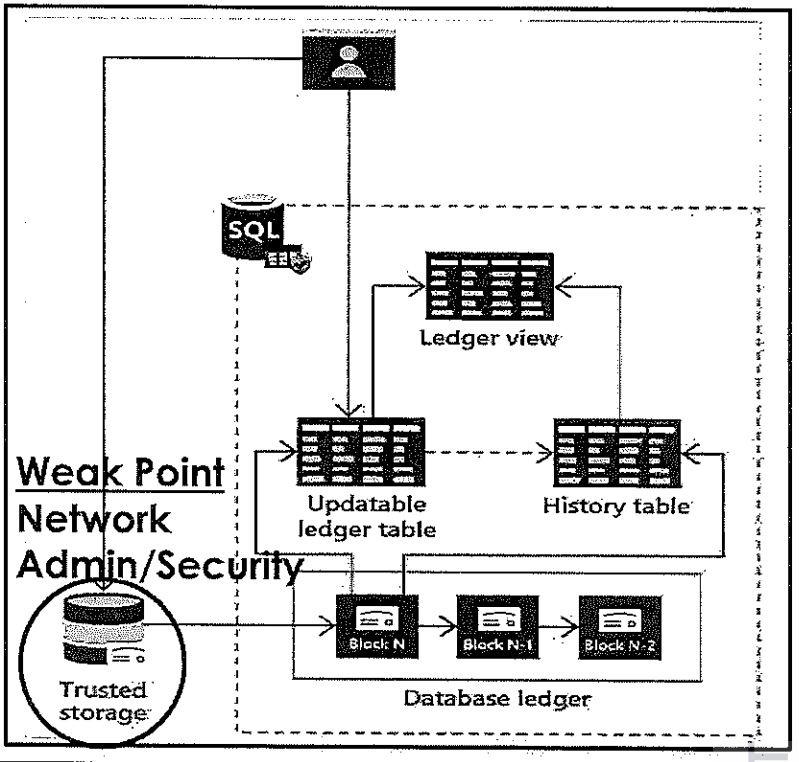
Voter registration info is housed in statewide databases that in many jurisdictions are created or maintained by a vendor

Maintaining trust requires:

- **Combination of security controls to reduce potential attacks**
- **Backup recover and restore practices**
- **Thorough disaster recovery procedures**

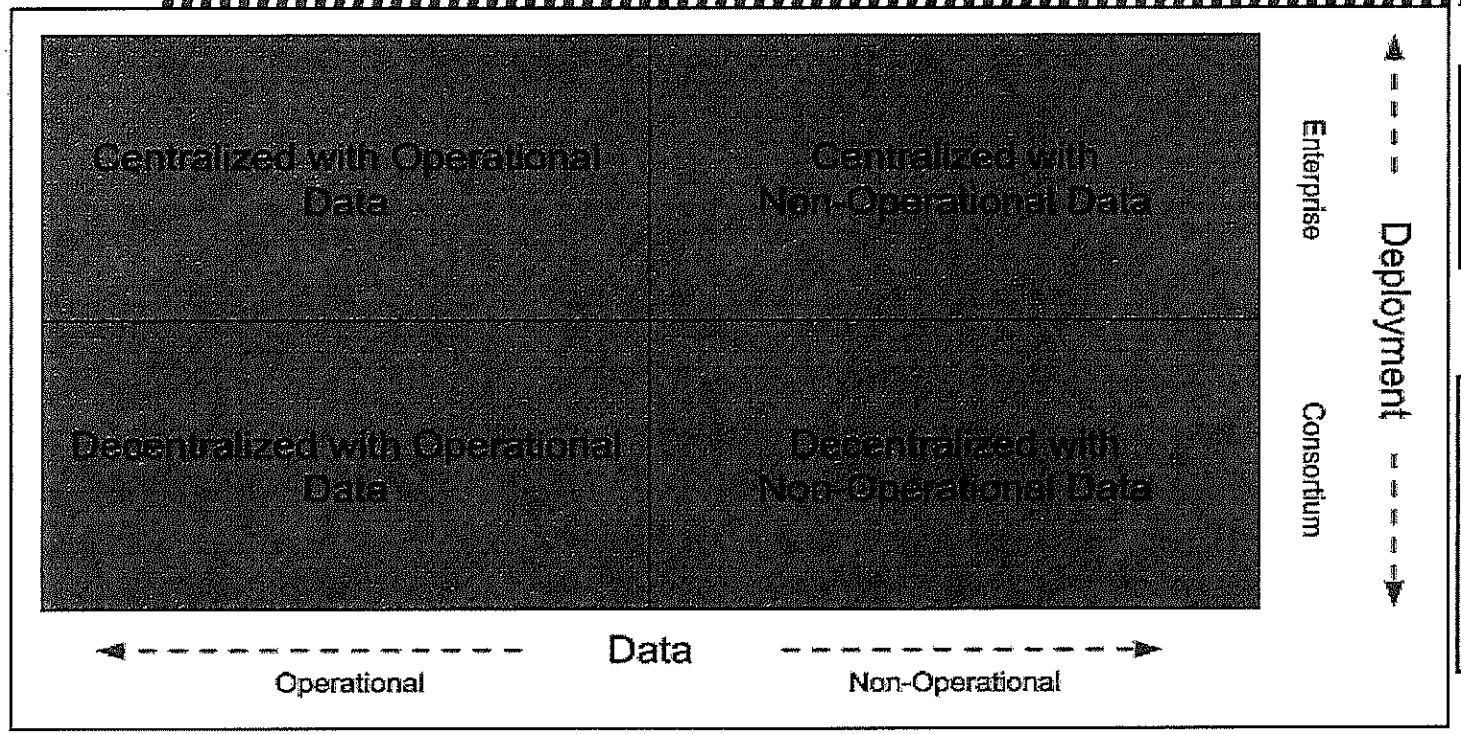
- **Updatable ledger tables** stores entry for every transaction and tracks the history of changes
- **History tables** automatically store the previous version of row **(i.e. commit, timestamp, & identity who executed it)**
- **Ledger Verification** doesn't allow modifying the content

Attacker can edit database files in storage bypassing system checks and directly tamper with data



Ledger is Unable to Prevent Attacks; Guarantees Any Tampering will be Detected and Determined Through System-Wide Audit

Blockchain Digital Ledger - Deployment Configurations



Enterprise **uses a blockchain internally and acts as central authority controlling data *[SoS]***

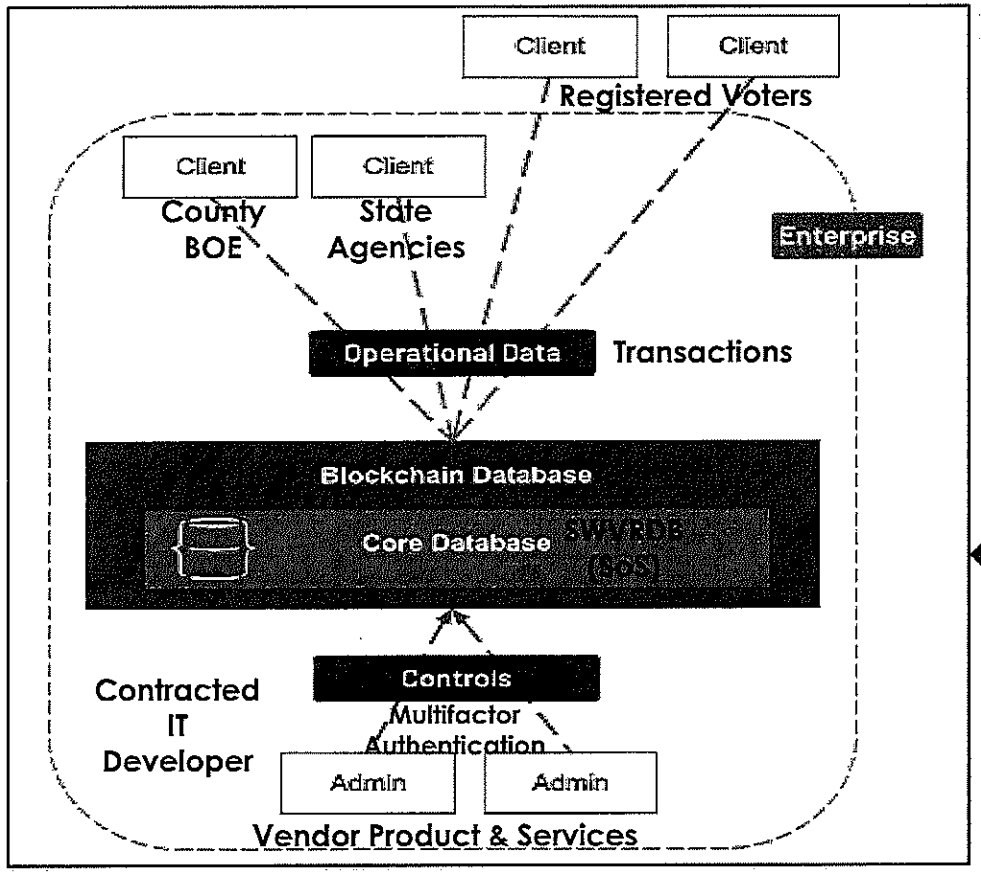
Consortium **ensures no single source owns the data, each validation node has copy of the data *[SoS / State Agencies / Registered Voters***

Operational vs. Non-Operational Data

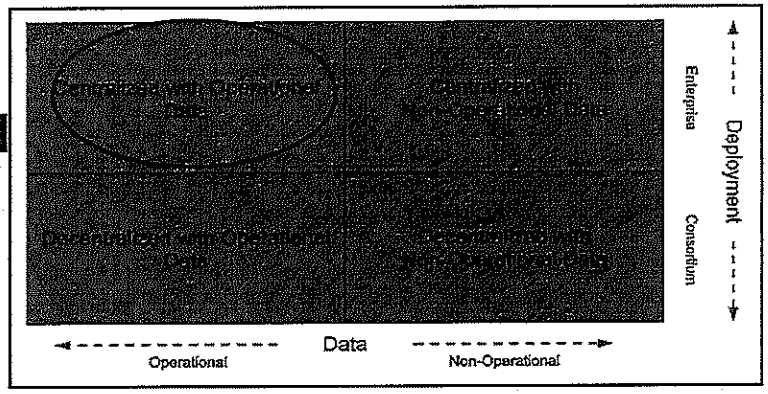
- Data used directly by clients connecting to database is referred to as operational data

Building Blockchain Database Depends on Determining Deployment Scenario and Data Use

Blockchain Use Case – Centralized with Operational Data

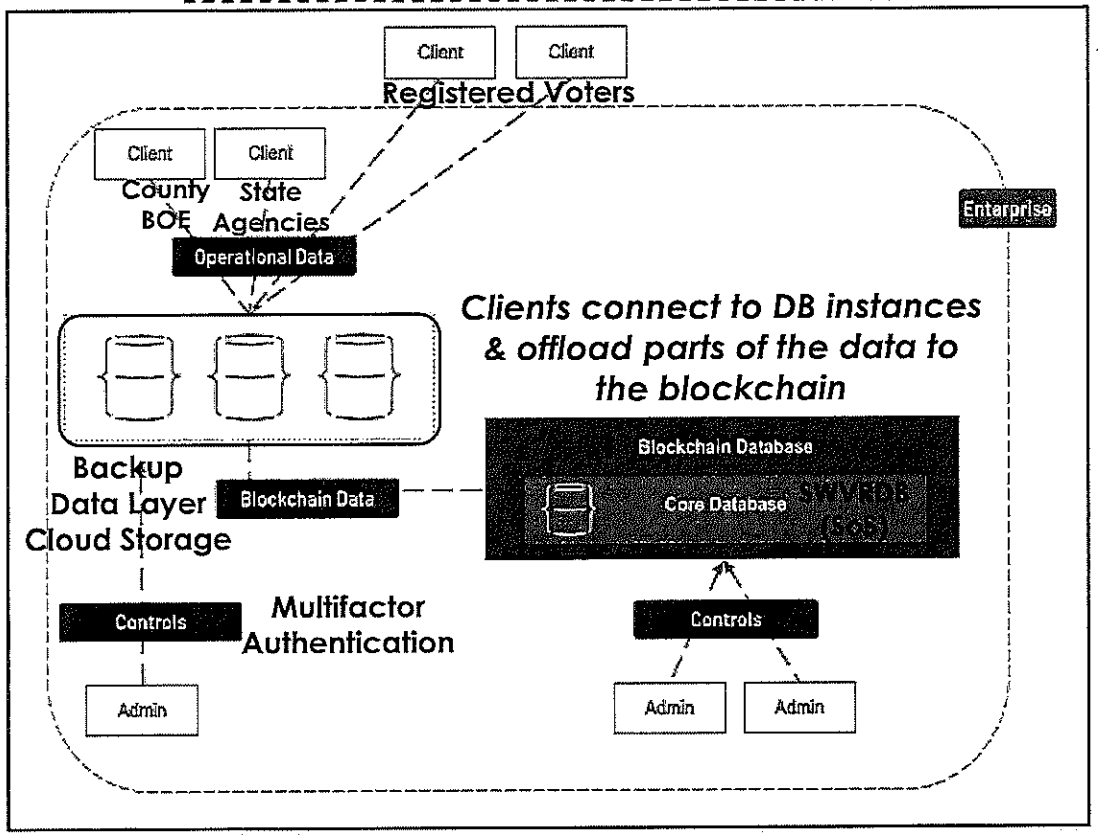


- Deployed within an enterprise ***(SoS/County BOEs)***
- **Provides immutability of documents** created and the **possibility to create and transfer assets**
- Familiar to most developer teams



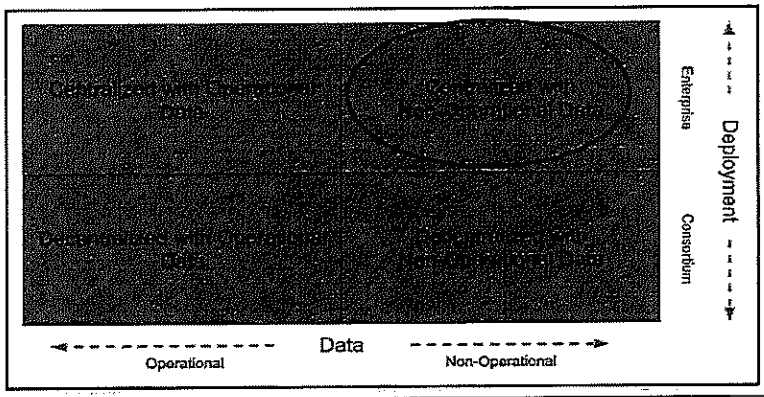
Requires Centralized Mechanism for Authenticating and Authorizing Service and Interface Access

Blockchain Use Case – Centralized with Non-Operational Data



This deployment maintained by a number of administrators ***[Current SoS Model for SWVRDB]***

- ***Data is NOT accessed directly by clients*** (i.e. registered voters)
- ***Additional layer reduces the number of nodes*** needed to agree to accept transaction, increasing DB performance
- ***Adds more privacy*** since data is only ***accessible by a limited number of clients*** controlled by enterprise

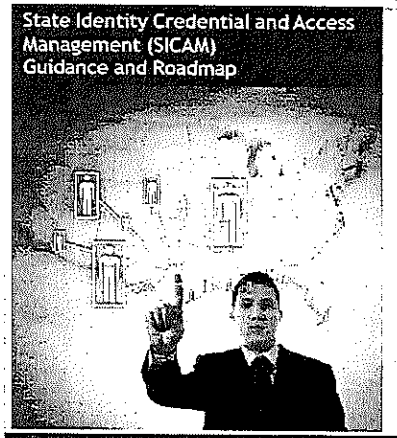


This Deployment Configuration Embraces Speed and Privacy

Security Model - Authentication and Authorization

Level of Discoverability	Definition
Public	Indicates that anyone can see the dataset record
Protected	Indicates the dataset record will be visible to all but only a subset of fields will be displayed
Private	Only the listed Access Control Groups and Users can see the record (If Private Record is selected, a reason must be provided)

Role	Access Privilege
Reader	The Reader can read records based on permissions
Editor	The Editor can read, create, and edit records based on permissions
Manager	The Manager has Editor access and can delete records and has option to recover or purge datasets
Group Access Control	The user can manage the membership and privileges of other users within access control grp



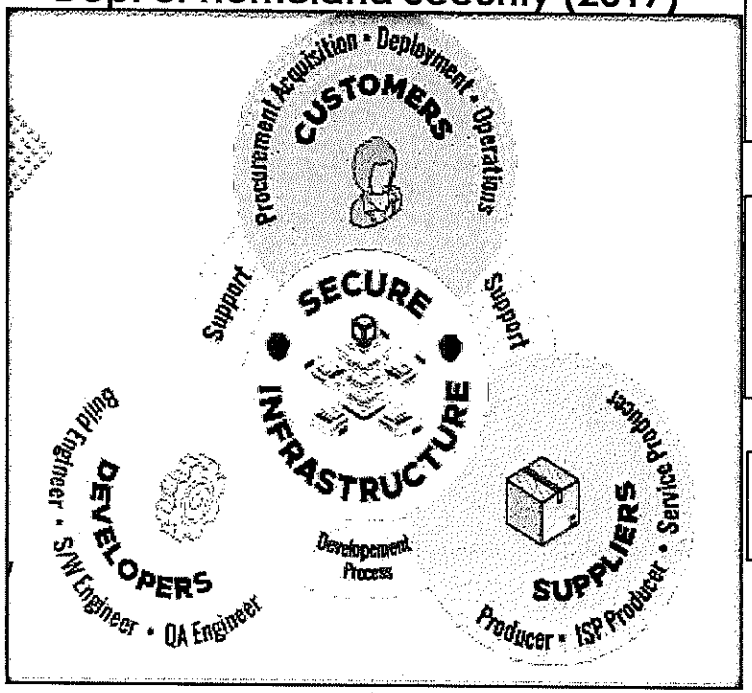
Blockchain is an opportunity to implement:

"States can provide a secure, auditable environment for the processing and exchange of information across entire spectrum of State business"

Blockchain Ledger is opportunity to implement State Identity and Credential Management (SICAM) Guidance

Ohio Voting System Certification – The Solution

Elections are
"National Critical Infrastructure"
-Dept of Homeland Security (2017)

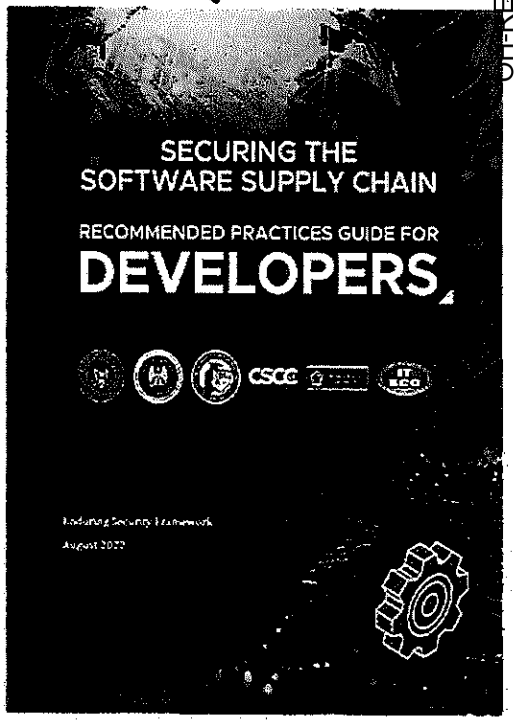


Codify following provisions into law:

1. ***Adopt Blockchain Digital Ledger Database on top of existing databases***

2. ***Vendors adhere to federal security development practices*** *and disclose voting system development practices* ***as condition of certification***

3. ***Introduce in-state 3rd party Independent Cyber Security Reviews***



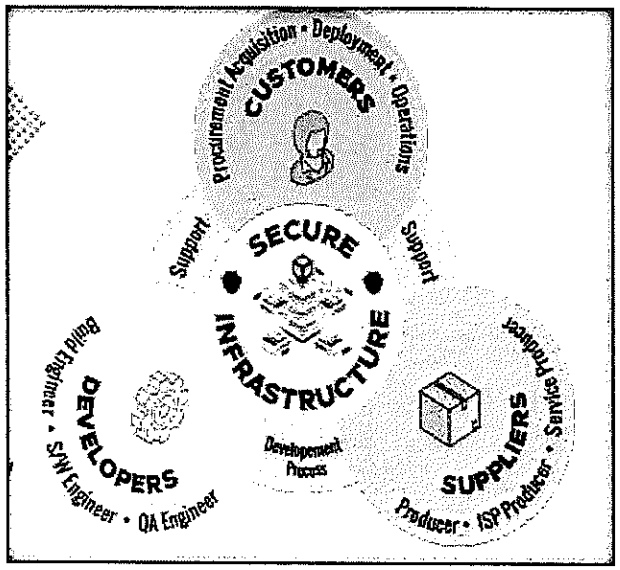
Empower OHIO CYBER RESERVE to lead certification security reviews in partnership with SOS as a pre-requisite to election voting system selection and County BOE procurement

Summary

Challenges

- ***No federal certification standards for most voting systems*** products and services
- Election systems ***continue to certify to obsolete 2005 security standards*** through 2023
- ***No election vendor oversight*** for software supply chain integrity & security development practices
- **Voter registration data is vulnerable and unable to securely track and protect data** from any attack or high privileged user

Recap



Questions?

Solutions

- **Adopt Blockchain Digital Ledger Database** on top of existing relational databases for SoS and Voter Registration supporting Agency Enterprise
- **Vendors shall adhere to federal security development practices**, disclose software byproducts (i.e. artifacts) & agree to 3rd party security review **as condition of certification**
- **Direct Ohio Cyber Reserve to conduct security analysis review** of election vendor systems

Hannum, Logan

Subject:	Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion
Location:	Microsoft Teams Meeting
Start:	Tue 6/4/2024 10:00 AM
End:	Tue 6/4/2024 10:30 AM
Show Time As:	Tentative
Recurrence:	(none)
Meeting Status:	Tentatively accepted
Organizer:	Hannum, Logan
Required Attendees:	Willis, Bernard; dauren.h.mason.nfg@army.mil; mstrbic@protonmail.com; Eberhart, Riley
SkypeTeamsProperties:	{"cid":"19:meeting_ZTg5YWM4ZTMtYzhhYy00Y2RlLWJiZGUtMjczNTU0NTc5Yzkw@thread.v2","rid":"0","mid":"0","private":true,"type":0}
SkypeTeamsMeetingUrl:	https://teams.microsoft.com/l/meetup-join/19%3ameeting_ZTg5YWM4ZTMtYzhhYy00Y2RlLWJiZGUtMjczNTU0NTc5Yzkw%40thread.v2/0?context=%7b%22Tid%22%3a%225fbc1338-b4f6-4a8f-91a9-43523a0b679f%22%2c%22Oid%22%3a%226145e2d3-0c79-4374-b47f-385e1650b72a%22%7d
SchedulingServiceUpdateUrl:	https://api.scheduler.teams.microsoft.com/teams/5fbc1338-b4f6-4a8f-91a9-43523a0b679f/6145e2d3-0c79-4374-b47f-385e1650b72a/19_meeting_ZTg5YWM4ZTMtYzhhYy00Y2RlLWJiZGUtMjczNTU0NTc5Yzkw@thread.v2/0
TeamsVtcTenantId:	5fbc1338-b4f6-4a8f-91a9-43523a0b679f
MeetingTemplateId:	default

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 255 398 727 065

Passcode: 3ozsaJ

Dial in by phone

+1 380-215-0572,,308674113# United States, Columbus

Find a local number

Phone conference ID: 308 674 113#

For organizers: Meeting options | Reset dial-in PIN

Hannum, Logan

From: Willis, Bernard
Sent: Monday, June 3, 2024 9:26 AM
To: Hannum, Logan; Marcell mstrbic
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Oh yeah, you told me that.... Well I say keep it for tomorrow. I will try to join, but really need Marcell on that Teams meeting to talk about the Cyber

Bunyan

Get Outlook for iOS

From: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Sent: Monday, June 3, 2024 9:08:47 AM
To: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

The issue is, he's on military leave from the 7-23 so not much time in between.

Get Outlook for iOS

From: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Sent: Monday, June 3, 2024 8:39:47 AM
To: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Would have to push it to the following Monday if possible..

Get Outlook for iOS

From: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Sent: Monday, June 3, 2024 8:07:47 AM
To: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Subject: RE: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Is there a time that would work better for you that you could be able to make it? Either way, I do think it would be a good idea for him to be in attendance.

-----Original Appointment-----
From: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Sent: Friday, May 31, 2024 8:12 PM
To: Hannum, Logan
Subject: Tentative: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion
When: Tuesday, June 4, 2024 10:00 AM-10:30 AM (UTC-05:00) Eastern Time (US & Canada).
Where: Microsoft Teams Meeting

I can't even be on Teams at that time, but do you think I should have Chachi (Lt Col Retired Marcell Strbich) attend?

Hannum, Logan

From: mstrbic <mstrbic@protonmail.com>
Sent: Monday, June 3, 2024 1:40 PM
To: Hannum, Logan
Cc: Willis, Bernard
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Logan,

Please send me the zoom link and your contact info for Tomm's 1000 mtg. I can lead HB 472 cyber security overview provisions with Cyber Reserve Reps.

-Marcell Strbich
937-607-4237

On Mon, Jun 3, 2024 at 9:25 AM, Willis, Bernard <Bernard.Willis@ohiohouse.gov> wrote:

> Oh yeah, you told me that.... Well I say keep it for tomorrow. I will try to join, but really need Marcell on that Teams meeting to talk about the Cyber
>
> Bunyan
>
> Get Outlook for iOS
>
> ---
>
> **From:** Hannum, Logan <Logan.Hannum@ohiohouse.gov>
> **Sent:** Monday, June 3, 2024 9:08:47 AM
> **To:** Willis, Bernard <Bernard.Willis@ohiohouse.gov>
> **Subject:** Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion
>
> The issue is, he's on military leave from the 7-23 so not much time in between.
>
> Get Outlook for iOS
>
> ---
>
> **From:** Willis, Bernard <Bernard.Willis@ohiohouse.gov>
> **Sent:** Monday, June 3, 2024 8:39:47 AM
> **To:** Hannum, Logan <Logan.Hannum@ohiohouse.gov>
> **Subject:** Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion
>
> Would have to push it to the following Monday if possible..
>
> Get Outlook for iOS
>
> ---
>
> **From:** Hannum, Logan <Logan.Hannum@ohiohouse.gov>
> **Sent:** Monday, June 3, 2024 8:07:47 AM
> **To:** Willis, Bernard <Bernard.Willis@ohiohouse.gov>
> **Subject:** RE: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Is there a time that would work better for you that you could be able to make it? Either way, I do think it would be a good idea for him to be in attendance.

-----Original Appointment-----
From: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Sent: Friday, May 31, 2024 8:12 PM
To: Hannum, Logan
Subject: Tentative: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion
When: Tuesday, June 4, 2024 10:00 AM-10:30 AM (UTC-05:00) Eastern Time (US & Canada).
Where: Microsoft Teams Meeting

I can't even be on Teams at that time, but do you think I should have Chachi (Lt Col Retired Marcell Strbich) attend?

Hannum, Logan

From: Hannum, Logan
Sent: Monday, June 3, 2024 1:54 PM
To: mstrbic
Cc: Willis, Bernard
Subject: RE: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Afternoon Marcell:

This meeting should be rather small in size. This is a prep meeting with our TAG liaison to really engage on the Cyber Security side of the bill. I am excited you will be able to join and will send the Teams link over to you here very shortly!

S & B

Logan J. Hannum MPS
Legislative Aide
Representative Bernard "Bunyan" Willis
House District 74

From: mstrbic <mstrbic@protonmail.com>
Sent: Monday, June 3, 2024 1:40 PM
To: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Cc: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Logan,

Please send me the zoom link and your contact info for Tomm's 1000 mtg. I can lead HB 472 cyber security overview provisions with Cyber Reserve Reps.

-Marcell Strbich
937-607-4237

On Mon, Jun 3, 2024 at 9:25 AM, Willis, Bernard <Bernard.Willis@ohiohouse.gov> wrote:

> Oh yeah, you told me that.... Well I say keep it for tomorrow. I will try to join, but really need Marcell on that Teams meeting to talk about the Cyber
>
> Bunyan
>
> Get Outlook for iOS

From: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Sent: Monday, June 3, 2024 9:08:47 AM
To: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

The issue is, he's on military leave from the 7-23 so not much time in between.

Get Outlook for iOS

From: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Sent: Monday, June 3, 2024 8:39:47 AM
To: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Would have to push it to the following Monday if possible..

Get Outlook for iOS

From: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Sent: Monday, June 3, 2024 8:07:47 AM
To: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Subject: RE: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Is there a time that would work better for you that you could be able to make it? Either way, I do think it would be a good idea for him to be in attendance.

-----Original Appointment-----
From: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Sent: Friday, May 31, 2024 8:12 PM
To: Hannum, Logan
Subject: Tentative: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion
When: Tuesday, June 4, 2024 10:00 AM-10:30 AM (UTC-05:00) Eastern Time (US & Canada).
Where: Microsoft Teams Meeting

I can't even be on Teams at that time, but do you think I should have Chachi (Lt Col Retired Marcell Strbich) attend?

Hannum, Logan

From: Willis, Bernard
Sent: Tuesday, June 4, 2024 10:11 AM
To: Hannum, Logan; mstrbic
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

My meeting in TX is starting concurrently with this one now. I will be on just in case

Get Outlook for iOS

From: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Sent: Monday, June 3, 2024 12:54:00 PM
To: mstrbic <mstrbic@protonmail.com>
Cc: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Subject: RE: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Afternoon Marcell:

This meeting should be rather small in size. This is a prep meeting with our TAG liaison to really engage on the Cyber Security side of the bill. I am excited you will be able to join and will send the Teams link over to you here very shortly!

S & B

Logan J. Hannum MPS
Legislative Aide
Representative Bernard "Bunyan" Willis
House District 74

From: mstrbic <mstrbic@protonmail.com>
Sent: Monday, June 3, 2024 1:40 PM
To: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Cc: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Logan,

Please send me the zoom link and your contact info for Tomm's 1000 mtg. I can lead HB 472 cyber security overview provisions with Cyber Reserve Reps.

-Marcell Strbich
937-607-4237

On Mon, Jun 3, 2024 at 9:25 AM, Willis, Bernard <Bernard.Willis@ohiohouse.gov> wrote:

Oh yeah, you told me that.... Well I say keep it for tomorrow. I will try to join, but really need Marcell on that Teams meeting to talk about the Cyber

Bunyan

Get Outlook for iOS

From: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Sent: Monday, June 3, 2024 9:08:47 AM
To: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

The issue is, he's on military leave from the 7-23 so not much time in between.

Get Outlook for iOS

From: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Sent: Monday, June 3, 2024 8:39:47 AM
To: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Subject: Re: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Would have to push it to the following Monday if possible..

Get Outlook for iOS

From: Hannum, Logan <Logan.Hannum@ohiohouse.gov>
Sent: Monday, June 3, 2024 8:07:47 AM
To: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Subject: RE: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion

Is there a time that would work better for you that you could be able to make it? Either way, I do think it would be a good idea for him to be in attendance.

-----Original Appointment-----
From: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Sent: Friday, May 31, 2024 8:12 PM
To: Hannum, Logan
Subject: Tentative: Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion
When: Tuesday, June 4, 2024 10:00 AM-10:30 AM (UTC-05:00) Eastern Time (US & Canada).
Where: Microsoft Teams Meeting

I can't even be on Teams at that time, but do you think I should have Chachi (Lt Col Retired Marcell Strbich) attend?

Hannum, Logan

From: mstrbic <mstrbic@protonmail.com>
Sent: Sunday, June 23, 2024 10:21 PM
To: Hannum, Logan; Rep Bernie Willis
Subject: HB 472 Presentation for OHCyR (Tues Mtg)
Attachments: Securing OHs Election Infrastructure_TAG Brief_ Jun 10 24.pptx

Logan

Please see attached presentation for this Tuesday's mtg with OHCyR. Let me know if you have any questions.

Thanks,
Marcell

Sent with Proton Mail secure email.

Eberhart, Riley

From: Willis, Bernard
Sent: Monday, March 25, 2024 4:13 PM
To: mstrbic
Cc: Gail Niederlehner; Jim Rigano; swiggam@gmail.com; Hannum, Logan; Peterson, Bob
Subject: Re: Buckeye Institute Introduction to Ohio Election Bill

I love it. Let's get together with them soon. Maybe we can set up a F2F meet after Easter?

Bunyan

Get Outlook for iOS

From: mstrbic <mstrbic@protonmail.com>
Sent: Sunday, March 24, 2024 10:19 PM
To: Willis, Bernard <Bernard.Willis@ohiohouse.gov>
Cc: Gail Niederlehner <ohio4truth@proton.me>; Jim Rigano <jim@rigano.net>; swiggam@gmail.com <swiggam@gmail.com>
Subject: Fw: Buckeye Institute Introduction to Ohio Election Bill

Representative Willis,

Senior Legal Fellow of Conservative Partnership Institute (CPI) Cleta Micthell has come out strong for the proposed Ohio Votes Count Act. She offered to broker an introduction to the Buckeye Institute President Robert Alt for bill proponency.

Support of the election bill from the States foremost conservative affiliated think tank would lend further credibility to legislators considering co-sponsorship should they take a public position or testify on the bill.

Please feel free to share this development with the Committee Chairman.

Thank you,
Marcell Strbich
Ohio Elections Study Collaborative

Sent with Proton Mail secure email.

------- Forwarded Message -------
From: mstrbic <mstrbic@protonmail.com>
Date: On Sunday, March 24th, 2024 at 11:55 PM
Subject: Buckeye Institute Introduction to Ohio Election Bill
To: Cleta Mitchell <cleta@cletamitchell.com>
CC: Bryson Davis <bryson@electionintegrity.network>, Eileen Watts <ewattsohio@gmail.com>, Jim Womack <james.k.womack@gmail.com>, Barry Chapman <bchapman@cox.net>, Gail Niederlehner <ohio4truth@proton.me>, Jim Rigano <jim@rigano.net>, Eileen Watts <ewatts@columbus.rr.com>, ws095@hotmail.com <ws095@hotmail.com>

Hi Cleta,

Great idea! Could you please broker an introduction to Robert Alt of the Buckeye Institute to myself, Eileen Watts, and former Ohio legislator advisor Bill Schuck? Would a conference call sometime this week be possible?

Our objectives for the meeting involve introducing the following-

- Highlights of OH's citizen-initiated pending election bill (Exec Summary Attached)
  - Existing OH voter registration verification and data validation deficiencies
  - Overview of voting system certification standards, State non-compliance & security deficiencies
- BMV disclosed findings on non-citizens possessing OH voter credentials (Attached)
- Pending SoS FOIA request for 2023 annual non-citizen audit results of Statewide Registration Database (Attached)

We really could benefit from partnering with the renowned Buckeye Institute for legal support, advise and advocacy in the coming weeks as multiple legislative and potential legal filings coalesce leading up to the 2024 election.

Thank you,
Marcell Strbich

Sent with Proton Mail secure email.

On Sunday, March 24th, 2024 at 7:15 AM, Cleta Mitchell <cleta@cletamitchell.com> wrote:

Oh wow! That's phenomenal!!

Your data about noncitizens - have you petitioned the SOS to remove those registrations specifically and submitted with documentation of noncitizen status?

Have you considered reaching out to Robert Alt at Buckeye Institute to represent the coalition and file suit to remove these and other new noncitizens asap?

I'd be happy to connect you with Robert. Let me know. Cleta

Cleta Mitchell, Esq.
Senior Legal Fellow
Conservative Partnership Institute

202.431.1950 (cell)
cleta@cletamitchell.com
www.whoscounting.us

On Mar 23, 2024, at 10:16 PM, mstrbic <mstrbic@protonmail.com> wrote:

Hi Cleta,

We'll definitely look to bring Ralph onboard. To answer your question, our efforts (OEIN) are independent of the United Sovereign Americans (USA); however, the provisions within our proposed election bill would solve many of the voter registration inaccuracies and subsequent registration and voting violations alleged in the complaint.

I've attached a 1-pg Executive Summary of a constituent written election bill that will drop in Ohio's House in early Apr. The Chairman of Government Oversight Accountability Committee Rep Bob Peterson agreed to co-sponsor with Rep Berni Willis. Both State House Speaker and Senate

President were apprised and receptive to bringing this election bill to a full vote in legislature when ready.

Of note, the bill proposes multiple 1st-in-the nation measures-

- State-directed independent 3rd party cyber security assessment reviews of voting systems as condition of certification in addition to EAC VVSG 2.0 standards

- Defined voting system certification standards based on most up to date federal software security development guidelines to include vendor voting system disclosure requirements

- Independent audits of Voter Registration Databases by Auditor of State

- Adoption of anti-tamper proof digital blockchain ledger functionality for Voter Registration Databases at both State and County level

- Voter registration data validation measures and identity and citizenship verification PRIOR to SoS acceptance on voter rolls (i.e. Not being done today – 267K+ illegals in Ohio)

- County opt-in provision for hand counted paper ballots in place of voting machines.

If you or other stakeholders are interested, we can provide a presentation.

Let me know.

Marcell Strbich
Ohio Election Research Collaborative (OEIN Affiliate)

Sent with Proton Mail secure email

Sent with Proton Mail secure email.

On Sunday, March 24th, 2024 at 7:15 AM, Cleta Mitchell <cleta@cletamitchell.com> wrote:

> Oh wow! That's phenomenal!!
>
> Your data about noncitizens - have you petitioned the SOS to remove those registrations specifically and submitted with documentation of noncitizen status?
>
> Have you considered reaching out to Robert Alt at Buckeye Institute to represent the coalition and file suit to remove these and other new noncitizens asap?
>
> I'd be happy to connect you with Robert. Let me know. Cleta
>
> Cleta Mitchell, Esq.
> Senior Legal Fellow
> Conservative Partnership Institute
>
> 202.431.1950 (cell)
> cleta@cletamitchell.com
> www.whoscounting.us

On Mar 23, 2024, at 10:16 PM, mstrbic <mstrbic@protonmail.com> wrote:

Hi Cleta,

We'll definitely look to bring Ralph onboard. To answer your question, our efforts (OEIN) are independent of the United Sovereign Americans (USA); however, the provisions within our proposed election bill would solve many of the voter registration inaccuracies and subsequent registration and voting violations alleged in the complaint.

I've attached a 1-pg Executive Summary of a constituent written election bill that will drop in Ohio's House in early Apr. The Chairman of Government Oversight Accountability Committee Rep Bob Peterson agreed to co-sponsor with Rep Berni Willis. Both State House Speaker and Senate President were apprised and receptive to bringing this election bill to a full vote in legislature when ready.

Of note, the bill proposes multiple 1st-in-the nation measures-

- State-directed independent 3rd party cyber security assessment reviews of voting systems as condition of certification in addition to EAC VVSG 2.0 standards

- Defined voting system certification standards based on most up to date federal software security development guidelines to include vendor voting system disclosure requirements

- Independent audits of Voter Registration Databases by Auditor of State

- Adoption of anti-tamper proof digital blockchain ledger functionality for Voter Registration Databases at both State and County level

- Voter registration data validation measures and identity and citizenship verification PRIOR to SoS acceptance on voter rolls (i.e. Not being done today – 267K+ illegals in Ohio)

- County opt-in provision for hand counted paper ballots in place of voting machines.

If you or other stakeholders are interested, we can provide a presentation.

Let me know.

Marcell Strbich
Ohio Election Research Collaborative (OEIN Affiliate)

Sent with Proton Mail secure email.

Eberhart, Riley

From: Eileen Watts <ewattsohio@gmail.com>
Sent: Monday, May 20, 2024 12:48 PM
To: State Senator Theresa Gavarone; State Senator Andrew Brenner; Willis, Bernard; Rep Bernie Willis; Peterson, Bob
Cc: Marcell Strbich; Gail Niederlehner; Jim Rigano
Subject: Meeting to Brief on HB 472

Follow Up Flag: Flag for follow up
Flag Status: Flagged

Ohio Election Integrity Network is inviting you to a scheduled Zoom meeting.

Topic: HB 472 briefing for Senators
Time: May 20, 2024 01:00 PM Eastern Time (US and Canada)

Join Zoom Meeting
https://zoom.us/j/95895789585?pwd=OXVIQjB0WnNuRmdNSStneDB5ZENNUT09

Meeting ID: 958 9578 9585
Passcode: 930912

One tap mobile
+13126266799,,95895789585#,,,,*930912# US (Chicago)
+16469313860,,95895789585#,,,,*930912# US

Dial by your location
- **+1 312 626 6799 US (Chicago)**
- **+1 646 931 3860 US**
- **+1 929 436 2866 US (New York)**
- **+1 301 715 8592 US (Washington DC)**
- **+1 305 224 1968 US**
- **+1 309 205 3325 US**
- **+1 689 278 1000 US**
- **+1 719 359 4580 US**
- **+1 253 205 0468 US**
- **+1 253 215 8782 US (Tacoma)**
- **+1 346 248 7799 US (Houston)**
- **+1 360 209 5623 US**
- **+1 386 347 5053 US**
- **+1 507 473 4847 US**
- **+1 564 217 2000 US**
- **+1 669 444 9171 US**
- **+1 669 900 6833 US (San Jose)**

Meeting ID: 958 9578 9585
Passcode: 930912

Find your local number: https://zoom.us/u/ah46AKgdL

Eileen Watts
ewattsohio@gmail.com
614-352-1010

Eberhart, Riley

From: mstrbic <mstrbic@protonmail.com>
Sent: Monday, May 20, 2024 2:23 PM
To: Eileen Watts
Cc: State Senator Theresa Gavarone; State Senator Andrew Brenner; Willis, Bernard; Rep Bernie Willis; Peterson, Bob; Gail Niederlehner; Jim Rigano
Subject: Re: Meeting to Brief on HB 472 (Election Cybersecurity Bill)
Attachments: Securing Ohios Election Infrastucture_sept 2023.pdf; Securing OHs Voter Registration Systems_Oct 30th 2023.pdf

ALCON,

Please see the attached and preceding presentations prepared on your behalf in advance of your consideration for sponsorship of this critical election security legislation.

- Attachment #1: Securing Ohio's Election Infrastructure (3rd Party Security Reviews)
- Attachment #2: Securing Ohio's Voter Registration Systems (Blockchain)

Both presentations were given to the OH SoS and House Members in advance of legislative sponsorship of H.B. 472 The Ohio Votes Count Act (3 Apr 2024). Proponent testimony is scheduled this Wed (22 May/1100) in the House Homeland Security Committee chaired by Rep Haraz Ghanbari.

Thank you,
Marcell Strbich

Sent with Proton Mail secure email.

On Monday, May 20th, 2024 at 12:47 PM, Eileen Watts <ewattsohio@gmail.com> wrote:

> **Ohio Election Integrity Network is inviting you to a scheduled Zoom meeting.**
>
> **Topic: HB 472 briefing for Senators**
> **Time: May 20, 2024 01:00 PM Eastern Time (US and Canada)**
>
> **Join Zoom Meeting**
> **https://zoom.us/j/95895789585?pwd=OXVlQjB0WnNuRmdNSStneDB5ZENNUT09**
>
> **Meeting ID: 958 9578 9585**
> **Passcode: 930912**
>
> ---
>
> **One tap mobile**
> **+13126266799,,95895789585#,,,,*930912# US (Chicago)**
> **+16469313860,,95895789585#,,,,*930912# US**
>
> ---

Dial by your location
- **+1 312 626 6799 US (Chicago)**
- **+1 646 931 3860 US**
- **+1 929 436 2866 US (New York)**
- **+1 301 715 8592 US (Washington DC)**
- **+1 305 224 1968 US**
- **+1 309 205 3325 US**
- **+1 689 278 1000 US**
- **+1 719 359 4580 US**
- **+1 253 205 0468 US**
- **+1 253 215 8782 US (Tacoma)**
- **+1 346 248 7799 US (Houston)**
- **+1 360 209 5623 US**
- **+1 386 347 5053 US**
- **+1 507 473 4847 US**
- **+1 564 217 2000 US**
- **+1 669 444 9171 US**
- **+1 669 900 6833 US (San Jose)**

Meeting ID: 958 9578 9585
Passcode: 930912

Find your local number: https://zoom.us/u/ah46AKgdL

Eileen Watts
ewattsohio@gmail.com
614-352-1010

Securing Ohio's Election Infrastructure

A Legislative Approach and Cyber Security Perspective

Ohio Election Study Collaborative

Presenter: Marcell Strbich

September 8thth 2023

The views expressed are those of the individual only and not those of the U.S. Air Force or Dept of Defense

AMERICAN OVERSIGHT

Overview

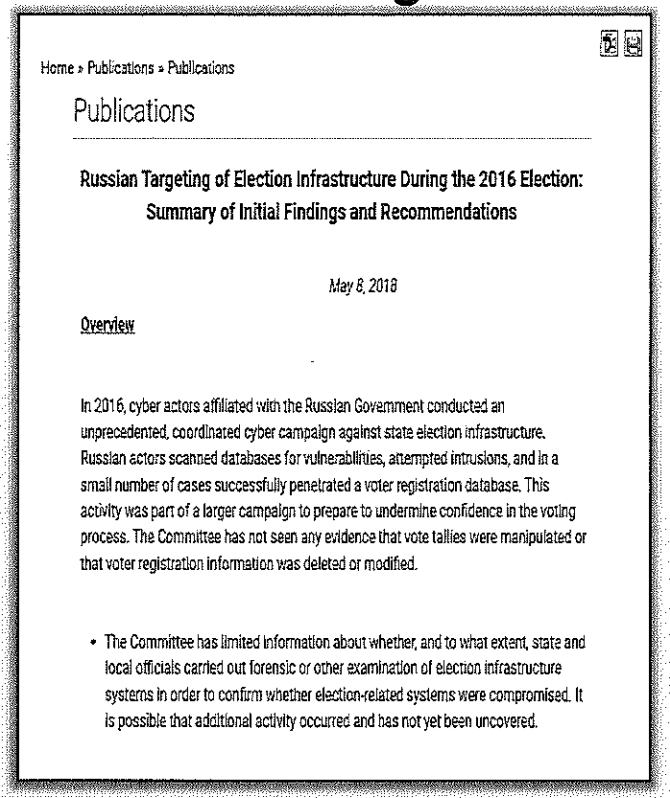
- Assessing Security Risk to Election Infrastructure
  - EO 14028 Improving the Nation's Cybersecurity
  - Election "Critical" Infrastructure Overview
  - Vendor – Products and Services Overview
- Federal Testing & Certification Process – The Problem
  - Voting System Certification – Issues & Challenges
  - Ohio Law Disconnect with Federal Law
- Current Ohio Election Security Measures – The Gap
  - Cybersecurity Functions Framework
  - Wireless Network Configuration – Patent Example
  - Current Law Vs. Standard – Election Systems
- Threats to Auditability - Ohio Use Case (DREs)
  - Computerized Voting Systems – Security Vulnerabilities
- National Resolution – Republican National Committee
  - Election Infrastructure – Cost Benefit Analysis
  - Ohio County BOE Engagement – Committee Report
  - Greene County – Opposing Resolution on DREs
  - Opt-Out Clause – Criteria & Alternatives
- Ohio Voting System Certification – The Solution
  - *Revised Ohio Law Security – Certification Provisions*
  - Vendor Certifiability – Requirement Standards
  - Summary – Recap and Questions

Assessing Security Risk to Election Infrastructure

Private Vendors play a central role in American elections ~ Prime Target

U.S. Senate Intelligence Committee Report (2018)

Publications | Intelligence Committee (senate.gov) –
Russian Targeting of Election Infrastructure



Home » Publications » Publications

Publications

Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations

May 8, 2018

Overview

In 2016, cyber actors affiliated with the Russian Government conducted an unprecedented, coordinated cyber campaign against state election infrastructure. Russian actors scanned databases for vulnerabilities, attempted intrusions, and in a small number of cases successfully penetrated a voter registration database. This activity was part of a larger campaign to prepare to undermine confidence in the voting process. The Committee has not seen any evidence that vote tallies were manipulated or that voter registration information was deleted or modified.

- The Committee has limited information about whether, and to what extent, state and local officials carried out forensic or other examination of election infrastructure systems in order to confirm whether election-related systems were compromised. It is possible that additional activity occurred and has not yet been uncovered.

Key Takeaway:

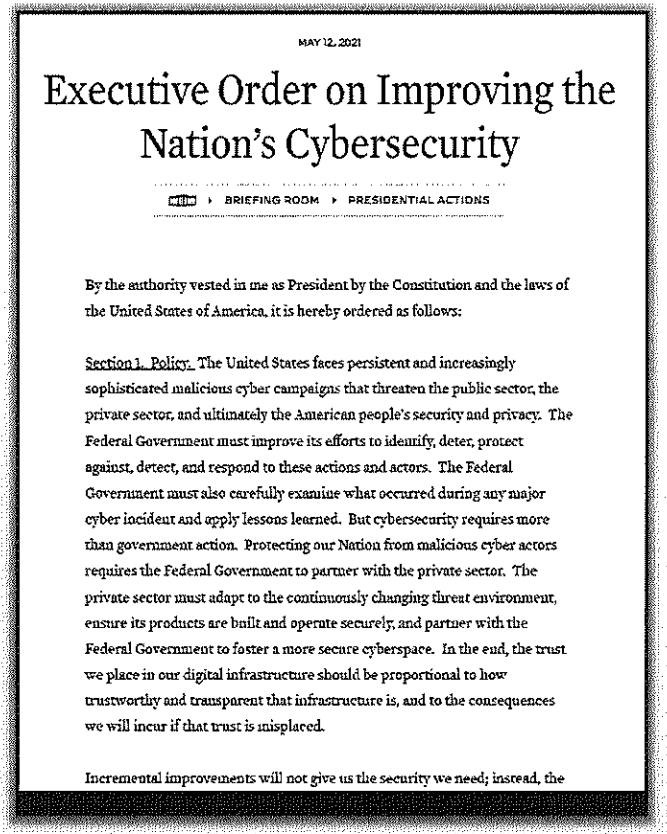
"State local, territorial, tribal, and federal government authorities have very little insight into the cyber security practices of [election] vendors"

Impossible to assess risk to vendors or impact to election security Without risk management framework

Executive Order 14028 – Improving the Nation's Cybersecurity (2021)

Key Highlights: Enhanced Vendor Risk Assessments

- **Growing emphasis on software security in supply chains**
- **Creates *higher standards for software verification techniques*** and other software ***supply chain controls***
- **Perform additional scrutiny on vendor Software Development Lifecycle (SDLC) capabilities,** security posture, and risks associated with Foreign Ownership, Control, or Influence (FOCI)



MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM › PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

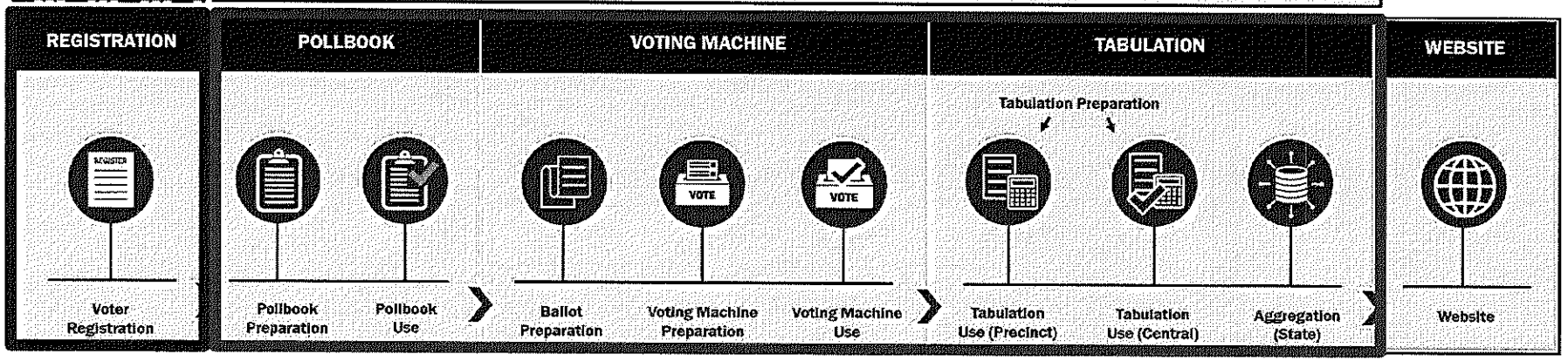
Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the

Federal government placing additional scrutiny on the software that vendors produce

Election "Critical" Infrastructure Overview

S.B. 14 Current scope of OH ***Board of Voting Machine Examiners*** equipment approval



Who has oversight of election vendors and authority to certify?

Where's the Critical Gap?

LIMITED TRANSPARENCY & ACCOUNTABILITY INTO VENDOR-DEVELOPER SECURITY PRACTICES

Ohio has opportunity to empower a State level Cyber security review team to conduct system security design and vulnerability verification

Vendor - Products and Services Overview

Vendors Present Points of Attack into Election Infrastructure

Voter Registration Database - No Federal or State certification standard

Voter registration info is housed in statewide databases that in many jurisdictions are created or maintained by a vendor.

Ballot Programming - No Federal or State certification standard

Prior to every election, voting machines must be programmed with a memory card or USB stick to display the ballot or read and count votes. Vendors provide the software.

Electronic Pollbooks – No Federal or State certification standard

On Election Day, poll workers in jurisdictions check in voters using electronic pollbooks, usually provided by a vendor.

Voting Systems – Only partial voluntary federal certification standards at federal level

Jurisdictions use a variety of voting machines, all provided by vendors.

Election Night Reporting - No Federal or State certification standard

On election night, the general public can view election results through reporting websites provided by vendors.

Postelection Audits - No Federal or State certification standard

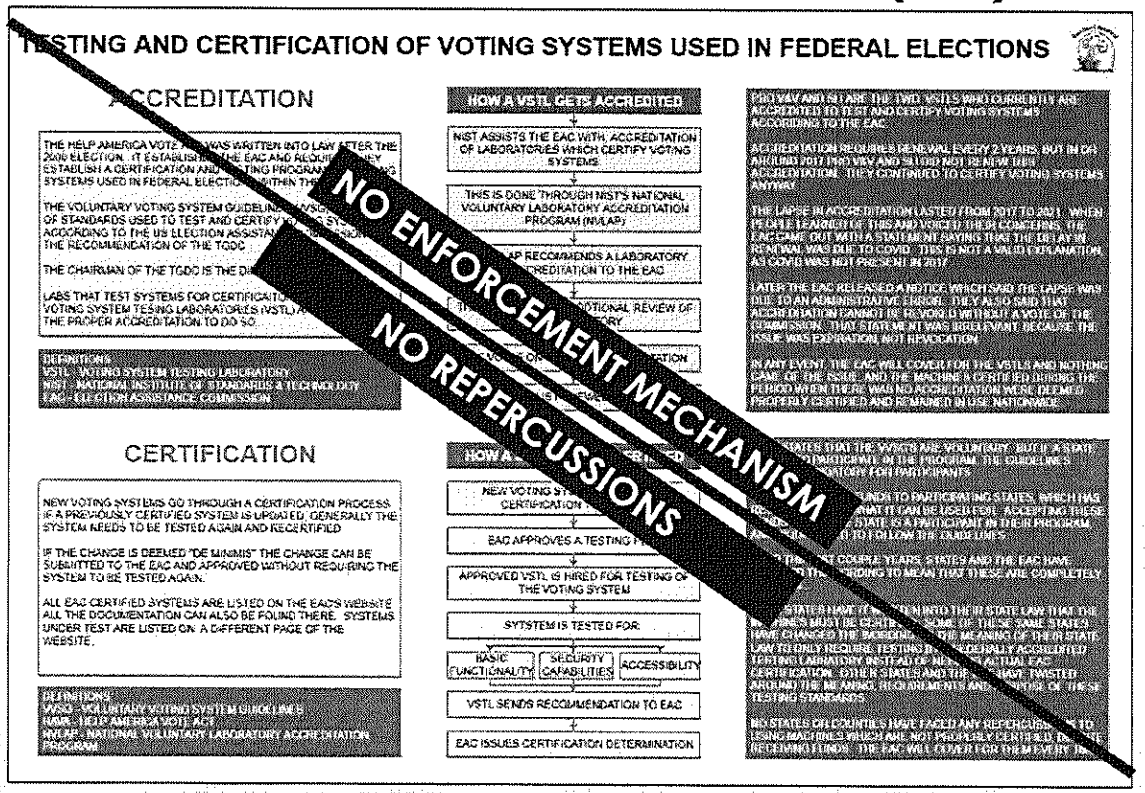
After an election, vendors and their equipment play a role in checking that the equipment and procedures used to count votes worked properly and that the election yielded the correct results.

Ohio law for voting machine certification based on federal voluntary guidelines

AMERICAN OVERSIGHT

Federal Testing & Certification Process – The Problem

Federal Election Assistance Commission (EAC)



<u>Questionable Vendor Affiliation Influence</u>

Only 2 National Voting System Labs

- Pro V&V & SLI
- Tests biased by manufacturer design, influence and funding

<u>Test Objectivity & Oversight Deficit</u>

- EAC lab accreditation delinquent 2017-2021
  - ***Voting systems still being certified to 2005 security standards (VVSG 1.0)***
  - Problems in multiple states (VA, NC, AZ)
  - No independent vendor cybersecurity attestation as criteria for certification

EAC does not have statutory authority to certify most election vendors

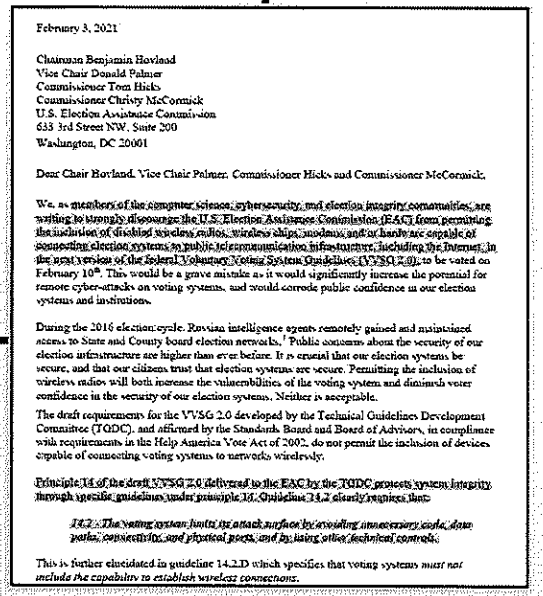
Voting System Certification Issues & Challenges

Computerized Voting System Security Vulnerabilities

EAC VVSG 2.0 standards will NOT mitigate ***known remote access threat***

25 leading computer science, cybersecurity & election integrity communities experts objected **to EAC inclusion of *disabled wireless radio, wireless chips, modems and/or hardware*** *capable* of connecting election systems to public telecom infrastructure in ***Voluntary Voting System Guidelines (VVSG 2.0)***

VVSG 2.0 Approval objection letter to Election Assistance Commission



February 3, 2021

Chairman Benjamin Hovland
Vice Chair Donald Palmer
Commissioner Tom Hicks
Commissioner Christy McCormick
U.S. Election Assistance Commission
633 3rd Street NW, Suite 200
Washington, DC 20001

Dear Chair Hovland, Vice Chair Palmer, Commissioner Hicks and Commissioner McCormick,

We, as members of the computer science, cybersecurity, and election integrity communities, are writing to strongly discourage the U.S. Election Assistance Commission (EAC) from permitting the inclusion of disabled wireless radios, wireless chips, modems, and/or hardware capable of connecting election systems to public telecommunication infrastructure, including the Internet, in the next version of the federal Voluntary Voting System Guidelines (VVSG 2.0), to be voted on February 10th. This would be a grave mistake as it would significantly increase the potential for remote cyber-attacks on voting systems, and would corrode public confidence in our election systems and institutions.

During the 2016 election cycle, Russian intelligence agents remotely gained and maintained access to State and County board election networks.[1] Public concerns about the security of our election infrastructure are higher than ever before. It is crucial that our election systems be secure, and that our citizens trust that election systems are secure. Permitting the inclusion of wireless radios will both increase the vulnerabilities of the voting system and diminish voter confidence in the security of our election systems. Neither is acceptable.

The draft requirements for the VVSG 2.0 developed by the Technical Guidelines Development Committee (TGDC), and affirmed by the Standards Board and Board of Advisors, in compliance with requirements in the Help America Vote Act of 2002, do not permit the inclusion of devices capable of connecting voting systems to networks wirelessly.

Principle 14 of the draft VVSG 2.0 delivered to the EAC by the TGDC protects system integrity through specific guidelines under principle 16. Guideline 14.2 clearly requires that:

14.2: The voting system limits the attack surface by avoiding unnecessary code, data paths, connectivity, and physical ports, and by using other technical controls.

This is further elucidated in guideline 14.2.D which specifies that voting systems *must not include the capability to establish wireless connections.*

EAC removed recommended prohibitions for wireless networking configuration

- **Permits networking capability** ⟷ ***"Grave mistake as it would significantly increase the potential for remote cyber-attacks on voting systems"***
- **Known remote system access methods-**
  - **Unintentional misconfiguration**
  - **A software update**
  - **Technical error**

Ohio law should require voting system equipment certification standards with greater rigor than EAC published VVSG 2.0

Ohio Law Disconnect with Federal Law

Current approved voting system certification standard is VVSG 2.0 (2021)

Certified Votings Systems	Election Assistance Commission Test & Certification Program		
Voting System (Name/Version)	Manufacturer	Testing Standard	Date Certified
Assure 1.2	Premier Election Solutions, Inc. (formerly Diebold Election Systems, Inc.)	VSS 2002	8/6/2009
ClearVote 2.1	Clear Ballot Group, Inc.	VVSG 1.0 (2005)	10/21/2019
ClearVote 2.2	Clear Ballot Group, Inc.	VVSG 1.0 (2005)	12/23/2021
ClearVote 2.3	Clear Ballot Group, Inc.	VVSG 1.0 (2005)	10/31/2022
Democracy Suite 4.14 Modification	Dominion Voting Systems Corp	VVSG 1.0 (2005)	7/18/2013
Democracy Suite 4.14-D Modification	Dominion Voting Systems Corp	VVSG 1.0 (2005)	11/25/2014
Democracy Suite 4.14-E Modification	Dominion Voting Systems Corp	VVSG 1.0 (2005)	7/2/2015
Democracy Suite 5.0	Dominion Voting Systems Corp	VVSG 1.0 (2005)	2/8/2017
Democracy Suite 5.0-A	Dominion Voting Systems Corp	VVSG 1.0 (2005)	8/14/2017
Democracy Suite 5.17	Dominion Voting Systems Corp	VVSG 1.0 (2005)	3/16/2023
Democracy Suite 5.5	Dominion Voting Systems Corp	VVSG 1.0 (2005)	9/14/2018
Democracy Suite 5.5-A (Modification)	Dominion Voting Systems Corp	VVSG 1.0 (2005)	1/19/2019
Democracy Suite 5.5-C	Dominion Voting Systems Corp	VVSG 1.0 (2005)	7/9/2020
Democracy Suite 5.5-D	Dominion Voting Systems Corp	VVSG 1.0 (2005)	6/8/2022

WHY NOT USE 2.0?

Sec. 3506.05 "Certification of Voting & Tabulating Equipment"

(H)(4)(a) "Any voting machine, marking device, or automatic tabulating equipment used in this state shall meet, ***as a condition of continued certification and use, the voting system standards adopted by the federal election commission in 2002 OR voluntary voting system guidelines most recently adopted by the election assistance commission."***

OH Law Disconnect

National Association of State Election Directors:

"Voting systems certified to the [old standard] will remain federally certified after November 15th 2023, and jurisdictions can continue using & purchasing those systems consistent with state laws and regulations." –Mar 2023

Source: U.S. Election Assistance Commission (eac.gov)-10 Aug 23

Transfer of voting system standards authority from FEC to the EAC under 2002 HAVA, supersedes Ohio's 2016 law citing FEC as system certification entity

Current Ohio Election Security Measures – The Gap

- In 2019, OH initiated a ***network security monitoring service*** w/DHS Center for Internet Security

  Special intrusion detection devices known as ***"Albert Sensors"*** installed across 88 counties

  **** Intent to identify malicious or potentially harmful network activity *"based on known signatures"***

  The Gap: Inability to detect poor practices and weak system design due to lack of visibility into vendors development security practices

  The Approach: Evaluate ***system security design upfront to discover system threats, vulnerabilities, malware and malicious software*** during *system production and build prior to customer delivery*

  *****No vendor directed by State to comply with security build practices as condition of certification***

Full cybersecurity unattainable without vendor security development practices disclosure

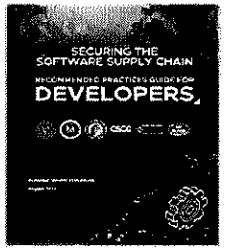
Cybersecurity Functions Framework

MISSING

CURRENT

Status of Voting System	Core Functions
• *In-Development*	• *Identify*
	• *Protect*
• Delivered	• Detect
• Fielded	• Respond
	• Recovery

Security review of vendor practices



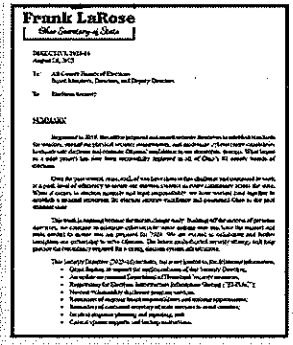
1 ***State Level Partnership (Certification)***

Collaboration

Ohio Cyber Reserve
+
Board of Voting Machine Examiners

2 Federal Level Partnership

End point security services (ESS)


Frank LaRose
Ohio Secretary of State

SoS Directive 2023-16 (Aug 28th 2023)

Collaboration

Ohio SoS
+
Dept of Homeland Security/
Center for Internet Security
*Crowdstrike (Vendor)

Ohio solves for *Detection, Responding & Recovering* but NOT *Identifying, Protecting*
The earlier security flaws are remediated in development, the less effort and cost

Wireless Network Connectivity Configuration – Patent Example

US009202113B2

(12) **United States Patent**
Hoover et al.

(10) **Patent No.: US 9,202,113 B2**
(45) **Date of Patent: *Dec. 1, 2015**

(54) **BALLOT ADJUDICATION IN VOTING SYSTEMS UTILIZING BALLOT IMAGES**

(71) Applicant: **Dominion Voting Systems, Inc.**, Denver, CO (US)

(72) Inventors: **James Hoover**, Outremont (CA); **Justin Bales**, Chula Vista, CA (US); **Steven Bennett**, Loma Linda, CA (US); **Eric Coomer**, Broomfield, CO (US); **Sean Dean**, Toronto (CA); **Genelon Mathews**, Golden, CO (US); **Benjamin Rice**, Brighton, CO (US)

(73) Assignee: **Dominion Voting Systems, Inc.**, Denver, CO (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/539,684**

(22) Filed: **Nov. 12, 2014**

(65) **Prior Publication Data**

US 2015/0071501 A1 Mar. 12, 2015

Related U.S. Application Data

(63) Continuation of application No. 13/470,091, filed on May 11, 2012, now Pat. No. 8,913,787.

(51) **Int. Cl.**

G06K 9/00	(2006.01)
G07C 13/00	(2006.01)
G06T 11/60	(2006.01)

(52) **U.S. Cl.**
CPC *G06K 9/00442* (2013.01); *G06T 11/60* (2013.01); *G07C 13/00* (2013.01); *G06T 2207/10004* (2013.01)

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2005/0247793	A1*	11/2005	Poulos et al.	235/386
2006/0041516	A1*	2/2006	Bogusky et al.	705/76
2010/0252628	A1*	10/2010	Chang	235/386

OTHER PUBLICATIONS

Premier Election Solutions. Premier Central Scan User's Guide, Revision 4.0. Jul. 9, 2009.*

* cited by examiner

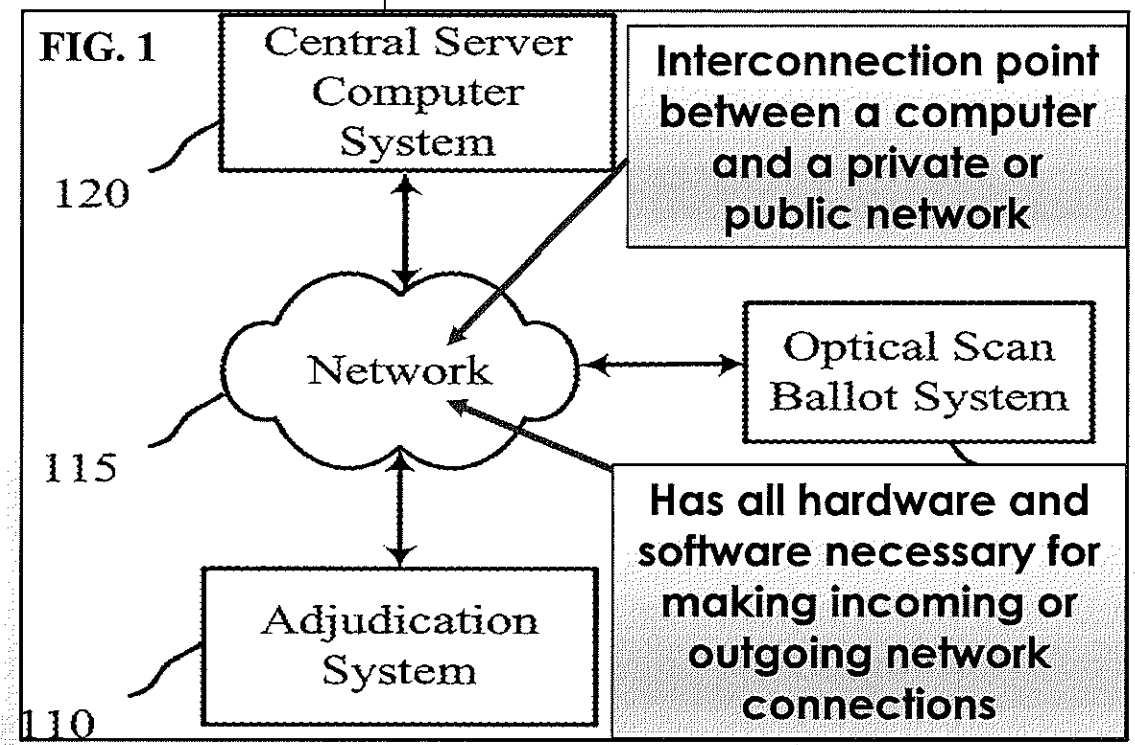
Primary Examiner — Niraj G Patel
(74) *Attorney, Agent, or Firm* — Holland & Hart LLP

(57) **ABSTRACT**

Methods, systems, and devices are described for adjudicating votes made on voter-marked paper ballots. Voter-marked paper ballots may be scanned to obtain optical image data of the voter-marked paper ballots. The optical image may be analyzed to determine the votes contained in the ballot for tabulation purposes. One or more votes on the ballot may be identified as requiring adjudication by an election official. Adjudication information, according to various embodiments, is appended to the optical images of the voter-marked paper ballots such that the image of the ballot and the image of the adjudication information may be viewed in an optical image. The optical image may be stored in a file format that allows the ballot image and the appended adjudication information to be viewed using readily available image viewers.

19 Claims, 16 Drawing Sheets

"May include multiple computers located locally and/*or remotely*"



While user can disable the wireless network from within the application, the user cannot disable the network interface on the device, the device's network card remains online and will send and receive

Current Law vs. Standard (Election Systems)

1 Ohio Law (2006) ⟷ **2 Ohio SoS Standard (2021)**

OHIO LAWS & ADMINISTRATIVE RULES
LEGISLATIVE SERVICE COMMISSION

HOME LAWS ABOUT CONTACT RELATED SITES GO TO

The Legislative Service Commission staff updates the Revised Code on an ongoing basis, as it completes its act review of during some times of the year, depending on the volume of enacted legislation.

Section 3506.23 | Voting machines not to be connected to internet.

Ohio Revised Code › Title 35 Elections › Chapter 3506 Voting And Tabulating Equipment

Previous Next

Effective: May 7, 2006 *Latest Legislation: House Bill 5 - 126th General Assembly* *PDF: Download Authenticated PDF*

A voting machine shall not be connected to the internet.

Ohio's current laws leave voting systems unprotected from cyber attacks

Ohio Voting System Requirements Matrix
Revised June 15, 2021

3. **Equipment has been certified by an independent testing authority as meeting or exceeding the minimum requirements of the U.S. Election Assistance Commission voting system standards (OAC 111:3-9-08(C)(15)).**

Acceptable ☐ Not Acceptable ☐

Covered in EAC Test Report/VSTL Test Materials? Yes ☐ No ☐ N/A ☐
Additional Information Concerning Testing Information:

Comments:

4. **A voting machine shall not be connected to the Internet (R.C. 3506.23). A voting system or voting machine is prohibited from containing any wireless communication hardware or software components.**

Acceptable ☐ Not Acceptable ☐

Covered in EAC Test Report/VSTL Test Materials? Yes ☐ No ☐ N/A ☐
Additional Information Concerning Testing Information:

Comments:

3 **Make Current SoS Rule OH Law:**
"A voting system or voting machine is prohibited from containing any wireless communication hardware or software components"

4 **Update Ohio law with Wireless Communication Restrictions:**
"Voting systems must not be capable of establishing wireless connections"

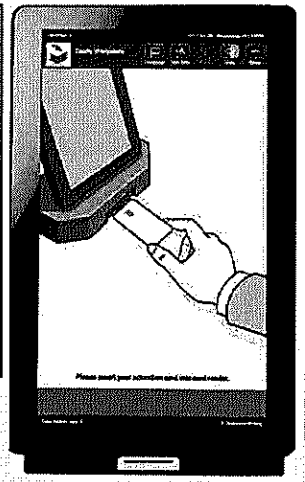
5 **As condition of certification, enforce security development practices & previous build activities disclosure requirements upon election system vendor-developers**

Threats to Auditability – Ohio Use Case (DREs)

- ***Touchscreen Direct Record Electronic (DRE) Voting Equipment***
  - ***Diminished verifiability creates auditing and federal compliance issue***
  - ***Deprive voters of the right to know-***
    - *"Election results are determined from Ballot QR codes, which malware can modify, yet voters cannot check that the QR codes match their intent, nor does the state compare them to the human-readable ballot text" – Halderman Report (2023)*

VOTING EQUIPMENT	COUNTY
Dominion Image Cast X (ADA) (direct recording electronic (DRE) with voter-verified paper audit trail (VVPAT))	Adams
	Butler
	Fairfield
	Greene
	Hancock
	Hardin
	Perry
	Richland
	Scioto
	Stark
	Wayne
	Wood

Ohio counties using DREs Voting Machines



Key Insights: Dominion ImageCast X Voting (DRE) Equipment

- *Scanners ignore the ballot text and count the votes encoded in the QR code not voter "Selection Summaries"*
- *QR code produces the cast vote record not the VVPAT, prohibiting HAVA Title III required auditability*
- Security design does not protect against duplicated QR codes or malware running on Ballot Marking Device (BMD)

Voter intent read from a QR code does NOT meet HAVA Title III 'Voting System Standards Manual Audit Capacity' requirement for auditable paper record

Computerized Voting Systems - Security Vulnerabilities

- ***Dominion ImageCast X (ICX) Ballot Marking Device (BMD)***
  - ***Principal Findings*** **– "ICX suffers from critical vulnerabilities" Altered both QR codes and human text**

Most Serious Vulnerabilities– (Halderman Report 2023)

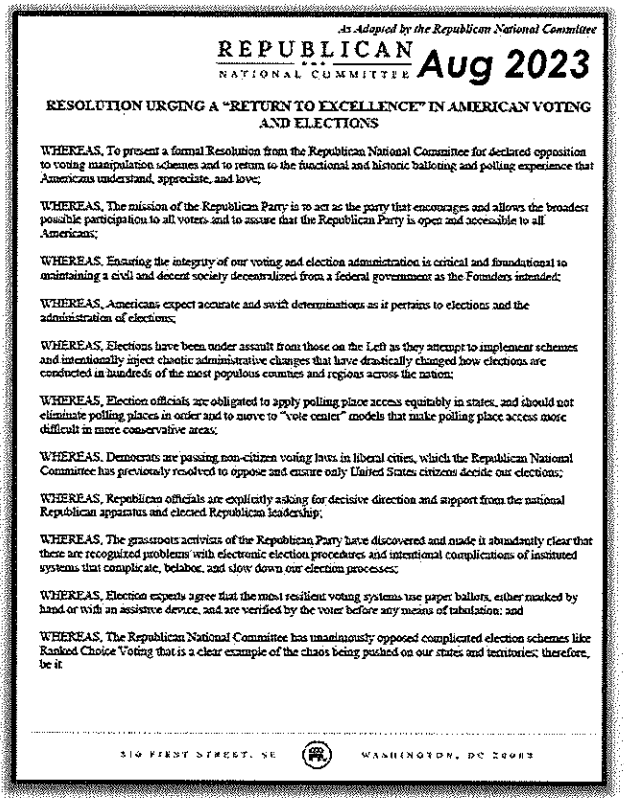
- Attackers ***altered QR codes on printed ballots*** to modify voters' selections
- ***Software updates*** lead to potential access/***malware install in polling place***
- ***Forged & manipulated smart cards*** used unlock any ICX and install malware
- ***Altered election definition*** **files** via arbitrary code***, can exploit all machines in the county***
- ***Access to scanner's memory card violate ballot secrecy*** by dishonest election worker
- Alteration of audit logs through access of ***unnecessary Android applications***
- ***Obtained county-wide keys via access to single ICX and Poll Worker Card & Pin,***
  - *All scanners & BMDs share same set of cryptographic keys for authentication*

Key Takeaway: ***BMDs and DREs in use in Ohio "developed without sufficient attention to security during design, software engineering and test…small mistake can lead to complete exploitation"***

BMDs and DREs are "not sufficiently secured to withstand vote-altering attacks"

National Resolution – Republican National Committee (RNC)

- "The grassroots activists…discovered and made abundantly clear ***there are recognized problems with electronic election procedures"***
- "**Election experts agree that the most resilient voting systems use paper ballots, …verified by the voter before means of tabulation"**
- "**RNC boldly opposes means of voting** that do not have proper safeguards…and are **exclusively electronic…*calls on every county and state in the nation to use default ballot systems, which are fully auditable, namely hand-marked, voter-verified paper ballots***
- "**RNC supports** the rights of **counties and states that** are willing and able to competently and efficiently **implement voting procedures that do no require the use of machines** and those **that implement hand counting procedures that are fully auditable"**
- "**RNC call on state legislatures, county, and municipal codes and rules that allow for full transparent hand-counting procedures that are planned, timely and fully observable"**
- "The **RNC calls on all Republican officeholders to defend…assigned precinct, ward and localized polling places for means of balloting and tabulating paper ballots by geographic unit"**



As Adopted by the Republican National Committee

REPUBLICAN NATIONAL COMMITTEE **Aug 2023**

RESOLUTION URGING A "RETURN TO EXCELLENCE" IN AMERICAN VOTING AND ELECTIONS

WHEREAS, To present a formal Resolution from the Republican National Committee for declared opposition to voting manipulation schemes and to return to the functional and historic balloting and polling experience that Americans understand, appreciate, and love;

WHEREAS, The mission of the Republican Party is to act as the party that encourages and allows the broadest possible participation to all voters and to assure that the Republican Party is open and accessible to all Americans;

WHEREAS, Ensuring the integrity of our voting and election administration is critical and foundational to maintaining a civil and decent society decentralized from a federal government as the Founders intended;

WHEREAS, Americans expect accurate and swift determinations as it pertains to elections and the administration of elections;

WHEREAS, Elections have been under assault from those on the Left as they attempt to implement schemes and intentionally inject chaotic administrative changes that have drastically changed how elections are conducted in hundreds of the most populous counties and regions across the nation;

WHEREAS, Election officials are obligated to apply polling place access equitably in states, and should not eliminate polling places in order and to move to "vote center" models that make polling place access more difficult in more conservative areas;

WHEREAS, Democrats are passing non-citizen voting laws in liberal cities, which the Republican National Committee has previously resolved to oppose and ensure only United States citizens decide our elections;

WHEREAS, Republican officials are explicitly asking for decisive direction and support from the national Republican apparatus and elected Republican leadership;

WHEREAS, The grassroots activists of the Republican Party have discovered and made it abundantly clear that there are recognized problems with electronic election procedures and intentional complications of instituted systems that complicate, belabor, and slow down our election processes;

WHEREAS, Election experts agree that the most resilient voting systems use paper ballots, either marked by hand or with an assistive device, and are verified by the voter before any means of tabulation; and

WHEREAS, The Republican National Committee has unanimously opposed complicated election schemes like Ranked Choice Voting that is a clear example of the chaos being pushed on our states and territories; therefore, be it

310 FIRST STREET, SE WASHINGTON, DC 20003

Resolution-Urging-a-Return-to-Excellence-in-American-Voting-and-Elections.pdf (gop.com)

Unanimous resolution calling State legislatures to pass laws allowing full transparent hand-counting procedures at precinct and local polling places for means of balloting and tabulation

Election Infrastructure – Cost Benefit Analysis

Butler County, Ohio ~ 1x Purchase Agreement $6.1M

- $6.1M X 88 Counties = ~ +$536M for Ohio Vendor Contracts

EXHIBIT A

TO THE VOTING SYSTEM AND SERVICES AGREEMENT
BY AND BETWEEN DOMINION VOTING SYSTEMS, INC.
AND THE COUNTY OF BUTLER, OHIO

PRICING SUMMARY AND DELIVERABLES DESCRIPTION

1. **Pricing Summary** - Prices of equipment, technical facilities, software, and other related services for voting, vote counting, and result processing. All pricing in U.S. Dollars.

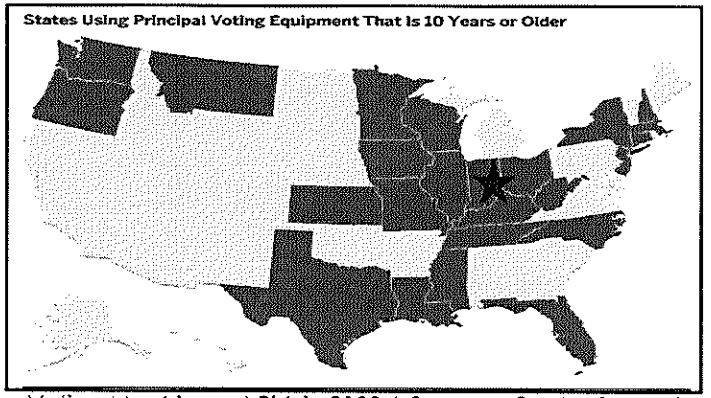
Table A: State-Funded Items pursuant to Exhibit C

DESCRIPTION	QTY	UNIT PRICE	EXTENSION PRICE
Central Scanning Solution: Absentee / Vote By Mail Hardware			
ImageCast Central Kit: Canon DR-G1130 high speed document scanner includes: ImageCast Central Software, Dell OptiPlex All-in-One, iButton programmer and key, cables	3	$ 25,000.00	$ 75,000.00
Sub-Total:			$75,000.00
In-Person Voting Solution: Polling Location Hardware			
ImageCast X DRE w/VVPAT (21 inch) Kit includes: ICX Firmware, Tablet, 5 voter activation cards, VVPAT, cables, power cord	1,500	$ 3,500.00	$5,250,000.00
ATI Accessible Voting Kit for ICX USB	100	$ 375.00	$37,500.00
ImageCast X Voting Log Stand	1,500	$250.00	$375,000.00
MBP System includes Oki Data C831E printer, laptop, cables	3	$11,560.00	$34,680.00
ICX Pollworker Smartcard	900	$ 8.00	$7,200.00
ICX Technician Smartcard	150	$ 8.00	$1,200.00
Dual Bay Battery Charger	50	$ 165.00	$8,250.00
8GB USB Flash Drive	1,500	$17.00	$25,500.00
Sub-Total:			$5,739,330.00
Election Management Hardware			
Democracy Suite EMS Express Server - up to 7 clients	1	$ 17,000.00	$ 17,000.00
EMS Client Workstation Configuration Kit	1	$ 2,500.00	$ 2,500.00
EMS Report Printer	2	$ 250.00	$ 500.00
Adjudication workstation	2	$1,900.00	$3,800.00
Smart Card Reader/Writer	5	$22.00	$110.00
Sub-Total:			$23,910.00
Software License Fee			
Democracy Suite (EMS) Application	1	$ 170,000.00	$ 170,000.00
Adjudication Software	1	$35,000.00	$35,000.00
Mobile Ballot Printing	1	$6,500.00	$6,500.00
			$211,500.00
Implementation Services	**Days**		
Voting System Deployment (e.g., software, installation & configuration, acceptance testing, etc.)	70	$ 2,000.00	$140,000.00

Dominion Voting Systems Inc.
Exhibit A – 5.16.2019

Butler County Purchase Agreement
Page 1 of 7

What is the <u>cost-benefit analysis</u> of an exclusively electronic voting system vs. blend of hand-marked paper ballot counting?



Voting Machines at Risk in 2022 | Brennan Center for Justice

Knowing computerized voting systems have known technical design security flaws and remote system threat access points enabled by activated wireless configuration that enable cyber exploitation and attack vulnerabilities….

How do we secure tens of millions of dollars worth of computerized voting system investment and restore public confidence without introducing real vendor accountability or oversight transparency of product development?

Reduce election system risk by requiring vendor-developers disclose system development security practices, foreign ownership and attest to software supply chain integrity

Ohio County BOE Engagement – Cost Benefit Analysis

17 August 2023

Greene County Republican Central Committee, Cost Benefit SubCommittee

Subject: Cost Benefit Analysis Committee Report **Aug 2023**

Purpose: The Cost Benefit Analysis Committee was formed to look into the costs associated with the voting machines versus paper.

Members: Katy Howard, Jo Tarka, Chip Sutton, Gary Tarka, James Johnson, Jan Basham, Frank Blackstone, Carolyn Uecker, Nancy Maxwell, and Anita Swan, Chair

We contacted the Director of the Greene County Board of Elections, Alisha Beeler Lambert, who gave us the background regarding the voting machines we currently use in Greene Country. The Dominion machines were procured in 2018 and put into service in 2019. They have a life expectancy of approximately 7-9 years. In addition to storage, testing and transportation expenses, there are annual licensing and maintenance fees associated with the voting machines. Greene County's population is approximately 168K.

We met with the Director of Clark County Board of Elections, Jason Baker. Clark Country uses only paper for their elections. Mr Baker was very gracious with his time and showed us the Clark Country voting process, the storage facilities and the tabulating process. Clark County's population is approximately 136K.

We also met with the Director of Montgomery County Board of Elections, Jeff Rezabek. Mr Rezabek was also very gracious with his time. Montgomery County uses both voting machines (ES&S) and paper during their elections, the voter selects which method to use. Mr Rezabek showed us the voting processes (paper and voting machines), storage and tabulating process. Montgomery Country recently conducted a cost comparison between using only paper or only machines for elections. The difference between the all paper versus all machines was significant (approximately $7.5M cost avoidance over a 10 year period). Montgomery County is recommending they move to all paper voting. Montgomery County's population is approximately 537K.

Note: If voting by paper ballot this requires a scanner/tabulator to "read" the ballot and tabulate the votes. These are not connected to the internet.

Conclusion: Both Montgomery County and Clark County have proven that the paper voting process is feasible and efficient. While the Montgomery County machines are different than the voting machines, we use here in Greene County we fully expect that there will be a large cost avoidance if Greene County moves to all paper voting rather than reprocuring and/or replacing/refurbishing our voting machines when the time comes. We recommend the Director of Greene County Board of Elections conduct a cost comparison between all paper voting versus machine voting and if, as expected, there is a significant cost avoidance, that Greene County move to all paper voting.

Respectfully,

Anita Swan, Chair, Cost Benefit Analysis Committee

- ***Engagement with Clark, Greene and Montgomery County BOEs***
  - Voting machine life expectancy 7-9 years (2019-2028)
  - Montgomery County cost benefit analysis between all paper and all machines indicated $7.5M cost savings over 10 years
    - "Montgomery County is recommending they move to all paper voting"

Recommendation: "We recommend the Director of Greene County BOE conduct a cost-comparison between all paper voting versus machine voting and if, as expected, there is a significant cost avoidance, that Green County move to all paper voting"

"Both Montgomery and Clark County have proven that the paper voting process is feasible and efficient"

Greene County - Opposing Resolution on DREs

Objectivity Deficit – Conflict of interest

- "Voting Machine contractor employees are involved in the audit and certification of their own machines before, during and after the election process"

Non-transparency – Questionable integrity of election process

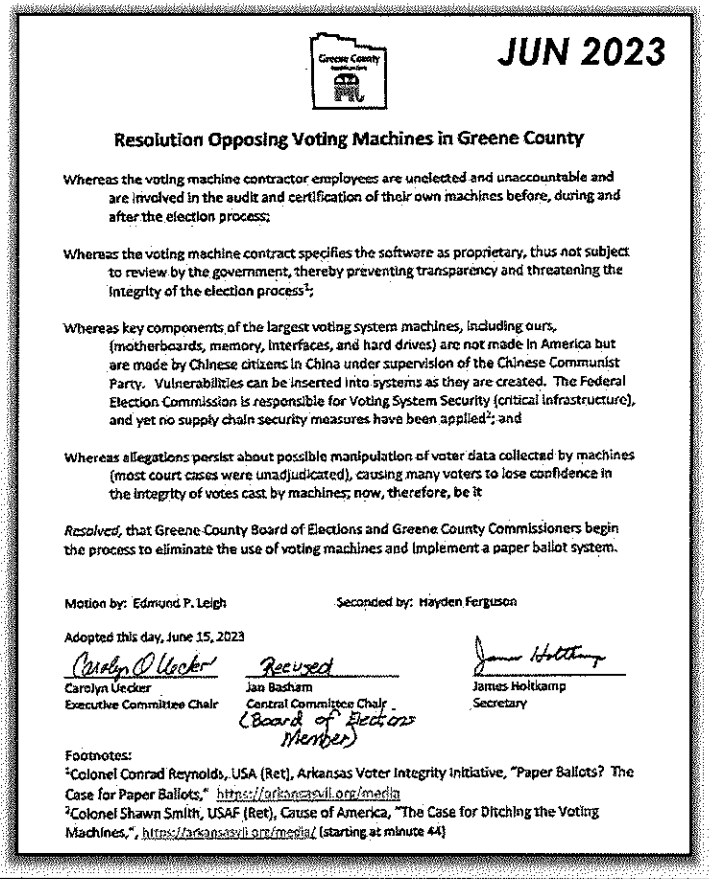
- "Voting machine contract specifies the software as proprietary, not subject to review by the government"

Supply chain integrity – Unaccounted and non-reviewable

- "Key components of voting system machines, (motherboards, memory, interfaces, and hard drives) are not made in America but made by Chinese citizens"
- "EAC is responsible for Voting system security and yet no supply chain security measures have been applied."

Public confidence in computerized voting systems decreasing

- "Allegations persist about possible manipulation of voter data (most court cases were unadjudicated), causing voters to lose confidence in integrity of votes cast by machines"



JUN 2023

Resolution Opposing Voting Machines in Greene County

Whereas the voting machine contractor employees are unelected and unaccountable and are involved in the audit and certification of their own machines before, during and after the election process;

Whereas the voting machine contract specifies the software as proprietary, thus not subject to review by the government, thereby preventing transparency and threatening the integrity of the election process[1];

Whereas key components of the largest voting system machines, including ours, (motherboards, memory, interfaces, and hard drives) are not made in America but are made by Chinese citizens in China under supervision of the Chinese Communist Party. Vulnerabilities can be inserted into systems as they are created. The Federal Election Commission is responsible for Voting System Security (critical infrastructure), and yet no supply chain security measures have been applied[2]; and

Whereas allegations persist about possible manipulation of voter data collected by machines (most court cases were unadjudicated), causing many voters to lose confidence in the integrity of votes cast by machines; now, therefore, be it

Resolved, that Greene County Board of Elections and Greene County Commissioners begin the process to eliminate the use of voting machines and implement a paper ballot system.

Motion by: Edmund P. Leigh Seconded by: Hayden Ferguson

Adopted this day, June 15, 2023

Carolyn Uecker
Executive Committee Chair

Received
Jan Basham
Central Committee Chair
(Board of Elections Member)

James Holtkamp
Secretary

Footnotes:
[1]Colonel Conrad Reynolds, USA (Ret), Arkansas Voter Integrity Initiative, "Paper Ballots? The Case for Paper Ballots," https://arkansasvii.org/media
[2]Colonel Shawn Smith, USAF (Ret), Cause of America, "The Case for Ditching the Voting Machines.", https://arkansasvii.org/media/ (starting at minute 44)

All voting systems face cybersecurity risks, not all voting systems are equally vulnerable

Opt-Out Clause: Criteria & Alternatives

Establish criteria to determine primary method for casting, recording & tabulating ballots in the event a voting systems fail certification standards:

Criteria Examples:

1. "All **components** have been **designed, manufactured, integrated and assembled in the U.S.** from trusted suppliers, using trusted processes accredited by the Defense Microelectronic Activity as prescribed by Dept of Defense
2. The **source code** used in any computerized voting machine for federal elections is **made available to the public or designated state directed cyber security review entity**
3. The **ballot images and system log files from each tabulator** are recorded on a secure write-once, read-many media with clear chain of custody and **posted on the Secretary of State's website** free of charge to the public within 24-72 hours after the close of polls

- Defense Microelectronics Activity - AccreditedSuppliers.pdf (osd.mil)

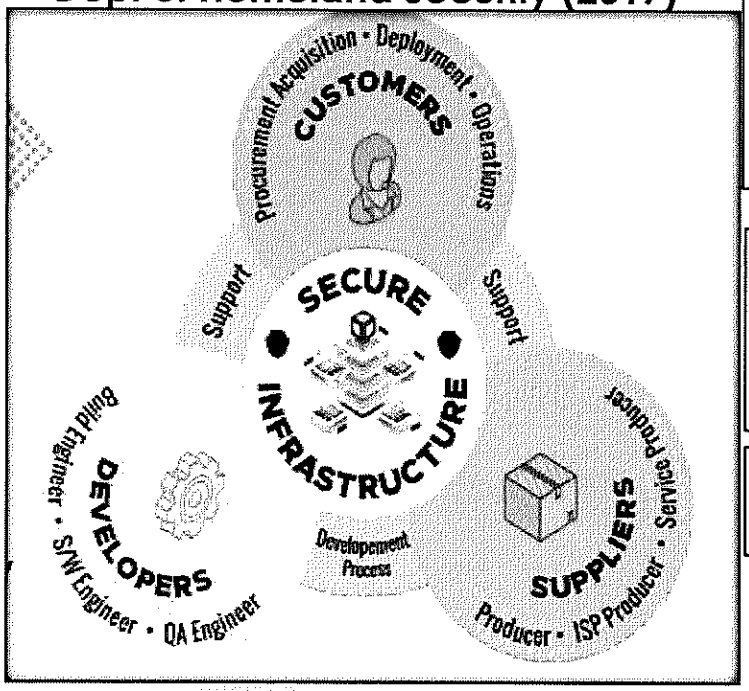
What will counties do if voting systems are de-certified?

Incorporate county machine-use opt-out provision into Sec 3506.05 in event of voting system de-certification?

Initiate a legislative study and/or county pilot project to study feasibility of primary hand-marked paper ballot counting at the precinct level

Ohio Voting System Certification – The Solution

Elections are "National Critical Infrastructure" -Dept of Homeland Security (2017)

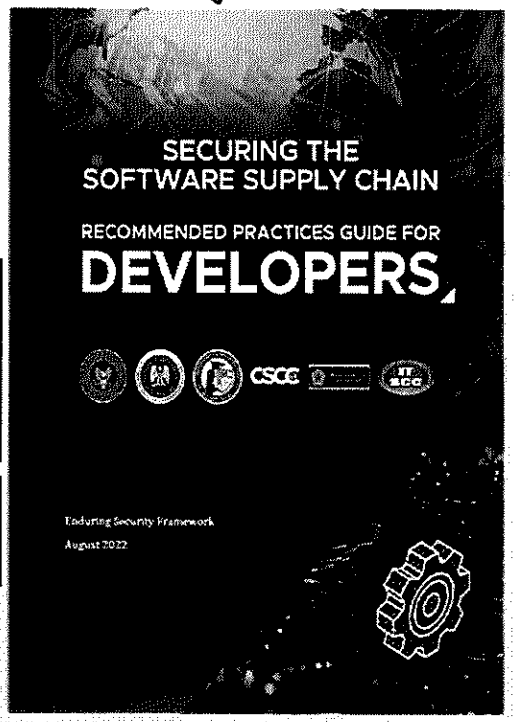


Codify following provisions into law:

1. ***Codify SoS system requirement rule*** prohibiting wireless hardware/software component in voting machines

2. ***Vendors adhere to federal security development practices*** *and disclose voting system development practices* ***as condition of certification***

3. ***Introduce in-state 3rd party Cyber Security Reviews***



Empower OHIO CYBER RESERVE to lead certification security reviews in partnership with SOS as a pre-requisite to election voting system selection and County BOE procurement

Revised Ohio Law - Security Certification Provisions

Vendor-Developer Provisions:

- **Adopt *software supply chain integrity security development best practices**
- **Require *security development build practices disclosure***
- ***Include background checks and security measures for personnel****
- ***Disclose vendor & subcontractor foreign ownership****
- ***Requirement and processes for reporting cyber incidents****
- ***Require Software Bill of Materials (SBOM)***
- **Accept recurring *State-directed 3rd party regular system build audits,*** penetration testing and physical site inspections
- ***Accept publication of system security review team findings on SoS website*** for public transparency

Brennan Center for Justice, "A Framework for Election Vendor Oversight: Safeguarding America's Election Systems (2019)

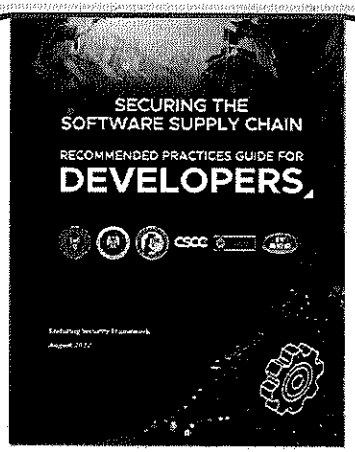
Update Section 3506.10 | Requirements for approval or certification of voting machines
Effective: May 7, 2004

Vendor Cyber Certifiability – Requirement Standards

Appendix D: Artifacts and Checklists

Producible Items
1. High-level Secure Development Lifecycle Process Document
2. Product Readiness Checklist
3. Product Support/Response Plan
4. Software Bill of Material (SBOM)
5. Architecture/Design Documents
6. Developer Training Certificates/Training Completion Statistics/data
7. Threat Model Results Document
8. High-level Software Security Test Plan and Results
9.Automatic and Manual Dynamic and Static Security/Vulnerability Reports (Security Scanning Results) Reports
10. Open Source Review Process Document and Allowed List
11. Build Log
12. Secure Development Build Configurations Listing
13. Third-Party Software Tool-Chains List

1



2

OHIO CYBER RESERVE
OhCR

Decision Point

Frank LaRose
Ohio Secretary of State

4

3

OH BOARD of VOTING SYSTEMS EXAMINERS

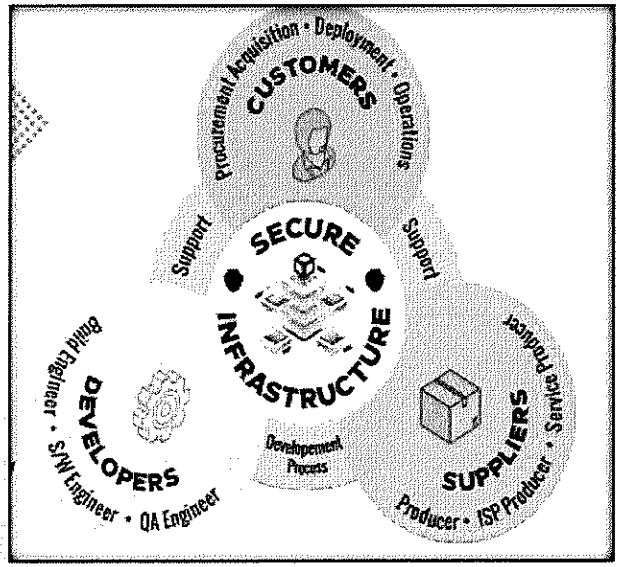
Ohio Cyber Reserve will perform cyber security verification of vendor-developer systems and submit report to OH SoS for Certification determination and public disclosure disclosure

Summary

Challenges

- ***No federal certification standards for most voting systems*** products and services
- Election systems ***continue to certify to obsolete 2005 security standards*** through 2023
- ***No election vendor oversight*** for software supply chain integrity & security development practices
- ***BMD and DRE voting machines not secured to withstand "vote altering attacks,"*** known threats can **falsify** voter intent & fail ***auditability under HAVA Title III via QR code***

Recap



Questions?

Solutions

- *Codify SoS system requirement rule prohibiting wireless hardware/software components* in voting machines
- **Vendors shall adhere to federal security development practices**, disclose software byproducts (i.e. artifacts) & agree to 3rd party security review **as condition of certification**
- **Direct Ohio Cyber Reserve to conduct security analysis review** of election vendor systems
- **Sunset DRE Voting Machines**, insufficiently secured, non-auditable
- **Specify County machine opt-clause for system de-certification** & hand-marked paper ballot counting pilot studies

Securing Ohio's Voter Registration Systems

A Legislative Approach and Cyber Security Perspective

Ohio Election Study Collaborative

Presenter: Marcell Strbich

October 30th 2023

The views expressed are those of the individual only and not those of the U.S. Air Force or Dept of Defense

Overview

- Overview Blockchain Upgrade
  - Ohio Sec of State - Legislation
  - Blockchain Opportunity – Ohio 1st in the Nation Status
- Cyber Security Core Functions Framework Review
  - Cyber Security – Attack Spectrum
  - Designated Agencies Providing Registration Services
- Blockchain Vs. Traditional Database Comparability
  - Voter Registration Database – Functional Design Limitations
  - Blockchain Digital Ledger Database – Features Explained
  - Blockchain Use Case - Overview
- Blockchain Digital Ledger – Deployment Configurations
  - Blockchain Use Case – Centralized with Operational Data
  - Blockchain Use Case – Centralized with Non-Operational Data
  - Security Model – Authentication and Authorization
- Ohio Voting System Certification – The Solution
  - Summary Recap

Overview - Blockchain Upgrade (Modernizing Databases)

Databases are software systems that store large collections of data for fast lookup, correlation, reporting, and retrieval by software application

Establishing trust around the integrity of data stored in database systems has been a longstanding problem for all organizations that manage sensitive data

Voter Registration Database data is vulnerable

Existing database lacks tamper resistance/ tamper evidence capabilities

Existing database lacks group validation and consensus mechanism to reduce risk of malicious alteration

Existing database does not preserve data value in maintained co-located history table

Existing data values and transactions do not utilize cryptographic security controls or multi-factor authentication for verification

Transformative Opportunity to Secure Voter Roll Integrity and establish System Wide Transparent Auditability for Proof of Malicious Data Alteration

Ohio Sec of State – Legislation

Frank LaRose
Ohio Secretary of State

DIRECTIVE 2023-16
August 28, 2023

To: All County Boards of Elections
Board Members, Directors, and Deputy Directors

Re: Elections Security

SUMMARY

Beginning in 2019, this office prepared and issued security directives to establish standards for vendors, strengthen physical security requirements, and modernize cybersecurity capabilities to ensure safe elections and continue Ohioans' confidence in our democratic process. What began as a pilot project has now been successfully deployed in all of Ohio's 88 county boards of elections.

Over the past several years, each of you have risen to this challenge and continued to work at a peak level of efficiency to secure our election systems in every community across the state. When it comes to election integrity and legal responsibility, we have worked hard together to establish a national reputation for election security excellence and positioned Ohio as the gold standard state.

This work is ongoing because the threats change daily. Building off the success of previous directives, we continue to prioritize cybersecurity while making sure you have the support and tools needed to ensure you are prepared for 2024. We are excited to collaborate and further strengthen our partnership to serve Ohioans. The below multi-faceted security strategy will help provide the redundancy required for a strong election system infrastructure.

This Security Directive (2023-16) includes, but is not limited to, the following information:

- Grant funding to support the implementation of this Security Directive;
- An update on required Department of Homeland Security resources;
- Registration for Elections Infrastructure Information Sharing ("EI-ISAC");
- No-cost vulnerability disclosure program services;
- Reminders of ongoing board responsibilities and training opportunities;
- Reminders of continued secretary of state services to assist counties;
- Incident response planning and reporting; and
- Critical system supports and backup instructions.

SoS Directive 2023-16 (Aug 28th 2023)

"We have worked hard together to establish a national reputation for election security excellence and positioned Ohio as the gold standard state"
–OH Sec of State Frank LaRose

Legislative Achievements [2019-2023]

- **S.B. 52 Creation of the Ohio Cyber Reserve Force**
- **H.B. 458 Voter Identification**
- **S.B. 51 Creation of Election Integrity Division**
- **S.B. 71 Data Analysis and Transparency Archives Act (DATA Act)**

Next:

- **Modernize Voter Registration System Certification Standards**
  - **Adopt Blockchain Digital Ledger Database**
  - **Vendor Security Development Practices Disclosure & 3rd party OH Cyber Reserve Security Assessments**

Prime Opportunity to Update Voter Registration System Certification Standards Into Legislation And Enact 3rd Party Security Reviews

Blockchain Opportunity – Ohio "1st in the Nation Status"

- **1st Voter Registration DB system to adopt Blockchain digital ledger database**
  - Securely track and protect data from any attacker or high privileged user ***(i.e. lock down voter rolls)***
  - *Capable of streamlined system-wide* ***auditing to reveal attestation proof for malicious attacks***

- **1st Voter Registration DB system to feature immutability and append-only features**
  - **Tamper Resistant:** Means difficult to reversibly change and impossible to overwrite data once stored
  - **Tamper Evidence:** Means once data is stored, any changes to it are easily detected
  - Operationalizes S.B. 14 Data Analysis Transparency and Analysis Archives Act (DATA Act)

- **1st State to require election vendors adhere to and report/disclose to 3rd party independent cyber security reviewers' security development practices as condition for State-level certification**
  - Codifies into law SoS Cybersecurity Directive 2023-16 (Aug '23), "establish standards for vendors"
  - Operationalizes S.B. 52 (2019) creating Ohio Cyber Reserve to protect critical election infrastructure

Blockchain Ledger DB Adoption ensures security controls and data integrity system-wide streamlined auditing

Cybersecurity Core Functions Framework Review

MISSING

Status of Voting System	Core Functions
• *In-Development*	• *Identify*
	• *Protect*

CURRENT

Status of Voting System	Core Functions
• Delivered	• Detect
• Fielded	• Respond
	• Recovery

Security review of vendor practices

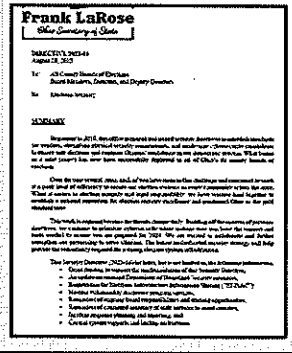
1 ***State Level Partnership (Certification)***

Collaboration

Ohio Cyber Reserve
+
Board of Voting Machine Examiners

2 Federal Level Partnership

End point security services (ESS)


Frank LaRose
Ohio Secretary of State

SoS Directive 2023-16 (Aug 28th 2023)

Collaboration

Ohio SoS
+
Dept of Homeland Security/
Center for Internet Security
*Crowdstrike (Vendor)

Ohio solves for *Detection, Responding & Recovering* but NOT ***Identify & Protect***
The earlier security flaws are remediated in development, the less effort and cost

Cyber Security – Attack Spectrum

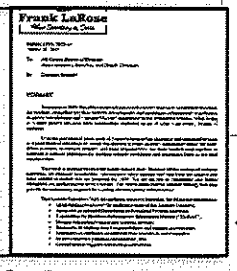
Application-Level Threats
- Input Validation Attacks
- Authentication and Authorization
- Data Exposure
- Business Logic Flaws

Software Development Life Cycle (SDLC) Threats
- Requirement Phase
- Design Phase
- Implementation Phase
- Testing Phase
- Deployment Phase
- Maintenance Phase

FEDERAL SECURITY PARTNERSHIP [DHS/OH SoS)

UPDATE STATE SECURITY LEGISLATION

Network Level Threats
- Perimeter Security
- Data Transmission
- ***Endpoint Security***
- Internal Threats


Frank LaRose

SoS Directive 2023-16
(Aug 28th 2023)

Frank LaRose
Ohio Secretary of State

Contractual Aspects Implications
- Security Requirements
- Compliance and Standards
- Liabilities and Indemnities
- Data Ownership and Privacy

Evaluate *network security at the access, application and data levels* for more secure, compliant and resilient operational environment

Designated Agencies Providing Registration Services

DATA ACT/2023

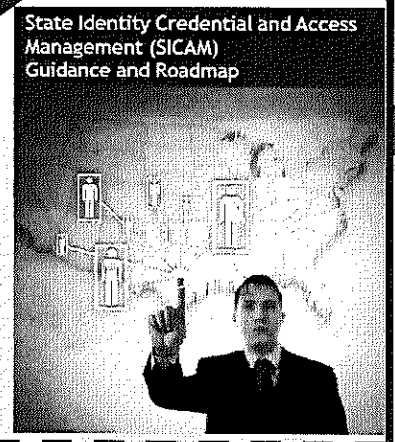
State Agencies – Database Maintenance

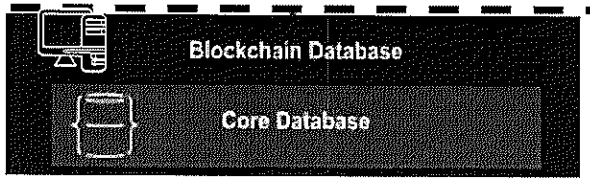
- Department of Health
- Bureau of Motor Vehicles
- Dept of Job and Family Services
- Dept of Medicaid
- Dept of Rehabilitation and Corrections

National Voter Registration Act (1993)

- Dept of Mental Health and Addiction Services
- Dept of Developmental Disabilities
- Opportunities for Ohioans with Disabilities
- *Ohio's four-year state-supported colleges and universities

*ORC Procedural Change

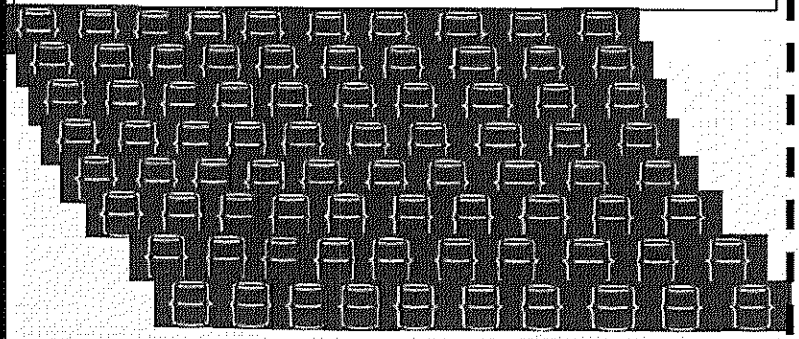




Statewide Voter Database [SOS]

County BOE Databases only interoperable with SoS Statewide Voter Registration Database, not State Agencies

88x County Board of Elections Databases



Blockchain Digital Ledger Database Enables Sharing, Verifying and Trusting Data Across Multiple-Party Business Processes Participating on the Network

Blockchain vs Traditional Database Comparability

	Blockchain	Databases
Data Integrity	The blockchain structure makes it virtually impossible for someone to change the data without breaking the chain. *[Anti-Tamper Evidence]*	A malicious actor can potentially alter data if necessary measures are not taken. *[No Tamper Evidence]*
Transactions	Data can only be read or added to the blockchain. *[Immutable-Irreversible]*	Data can be created, read, updated, or deleted (CRUD operations). *[Mutable-Reversible]*
Querying Performance	The verification methods to ensure data integrity can slow down the querying and general performance of a blockchain. *[Signed-Verified]*	Databases provide blazing-fast access to the data. *[No signature verification]*
Structure	Blockchains can be fully decentralized and not rely on any central authority. *[Transparency-Redundancy]*	Databases are centrally managed, and an administrator owns and controls the data. *[No practical data controls]*

Traditional Database (Relational)

Rigid Data Structure
- Used for well structured data
- Linked by relationships
- Lookup via common value
- Fast lookup results

Inflexible Development Options
- New fields require DB rebuild if software requirements for data changes
- Time-consuming and more expensive to upgrade apps

Auditing Impractical
- History not preserved in co-located way in database
- Unable to attest to alteration

Incorporating Blockchain On Top of Traditional Databases Retains Power, Flexibility and Performance and Adds Data Integrity

Voter Registration Database – Functional Design Limitations

- **Database is accessible** to a variety of IT and database administrator staff
  - **Data vulnerable** not only to abuse of privilege, but theft of this privilege and use by adversaries
  - **Threat surface is broad**; home-based, mobile personal computers or remote access by IT staff

- ***Transactions*** within the database are ***reversible*** and ***lack tamper-proof evidence*** capabilities
  - Any actor (authorized/unauthorized) that has obtained access can freely modify content of DB
  - ***Mutable data of*** voter records ***makes data integrity verification impractical and cumbersome***

- **Audit processes are highly time-intensive costly activities**
  - ***Changed values are overwritten, history not preserved in co-located manner*** *on the database*
  - **Unable to** perform streamlined system-wide audits or **provide attestable proof of malicious alteration**
  - ***No ability to replay or reconstruct voter roll transaction history***

Voter rolls (lists) are Stored in Traditional Relational Database Management Systems, With No Practical Controls on Data Integrity

Blockchain Digital Ledger Database - Features Explained

- **Adopts Decentralization: Transparency and Redundancy**
  - **Distributed database technology** allows data to be stored across a network of computers, rather than on a single centralized server

- **Adds Security Controls: Resistant to Cyber Attacks**
  - **Provides proof of data integrity to auditors**
  - **Adopts access control verification: Multifactor Authentication (MFA):**

- **Incorporates Immutability: Key to Public Trust and Transparency**
  - Once recorded, ***transaction is extremely difficult to alter or delete*** and is ***tamper-evident to all viewers (i.e Streamlines Auditing)***
  - ***Tampering*** will ***only be possible with collusion*** among multiple parties
  - Blockchain ledger is often ***accessible to the public, allowing anyone to view the transaction history [Optional]***

Blockchains Use Digital Ledgers to Securely Store Transactional Data and Verify Integrity Through Forensics and Playback Capabilities

Blockchain Use Case - Overview

Voter Registration Database - No Federal or State certification standard

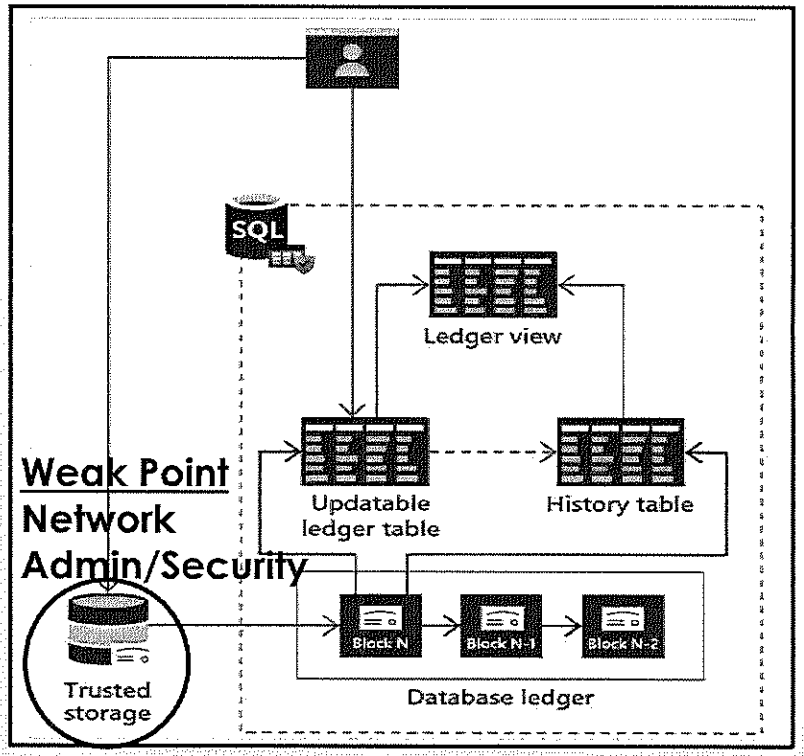
Voter registration info is housed in statewide databases that in many jurisdictions are created or maintained by a vendor

Maintaining trust requires:

- **Combination of security controls to reduce potential attacks**
- **Backup recover and restore practices**
- **Thorough disaster recovery procedures**

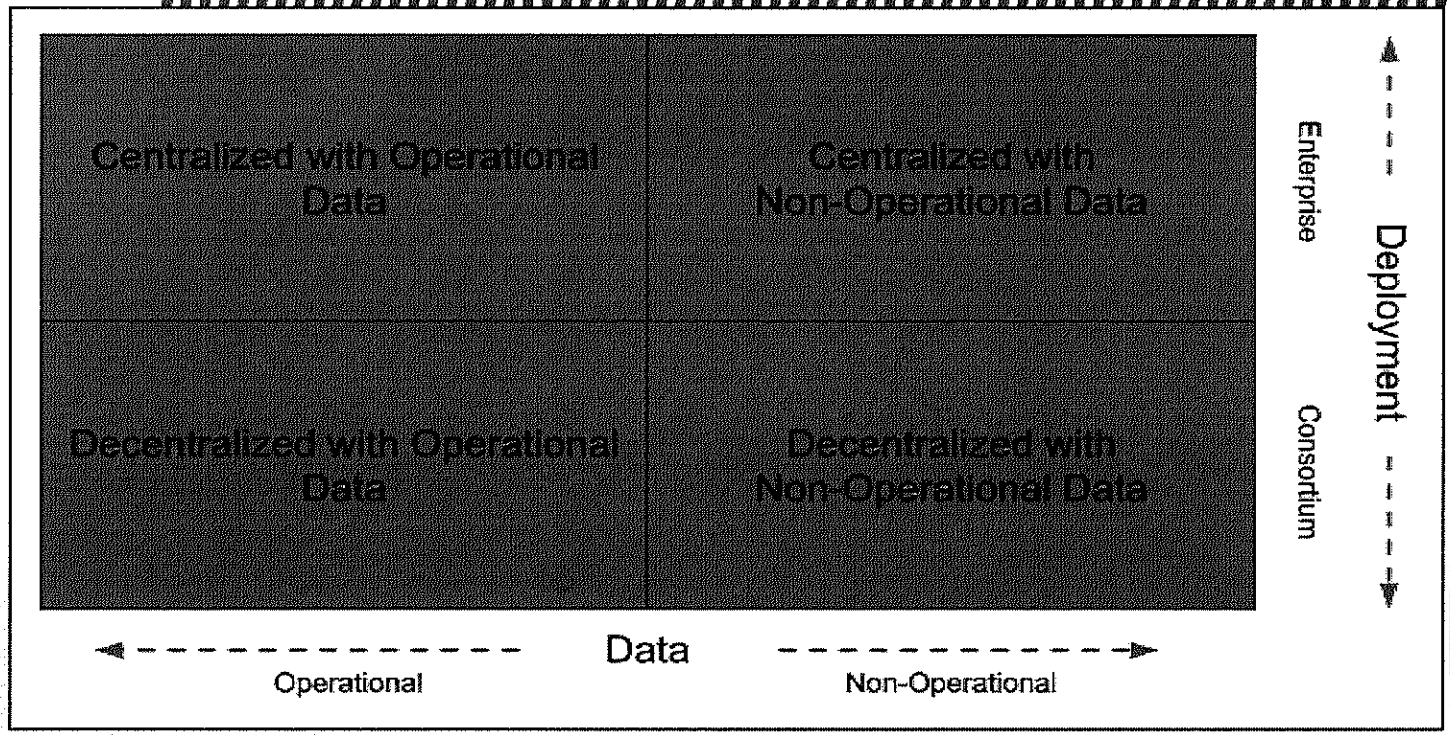
- **Updatable ledger tables** stores entry for every transaction and tracks the history of changes
- **History tables** automatically store the previous version of row **(i.e. commit, timestamp, & identity who executed it)**
- **Ledger Verification** doesn't allow modifying the content

Attacker can edit database files in storage bypassing system checks and directly tamper with data



Ledger is Unable to Prevent Attacks; Guarantees Any Tampering will be Detected and Determined Through System-Wide Audit

Blockchain Digital Ledger - Deployment Configurations



Enterprise **uses a blockchain internally and acts as central authority controlling data *[SoS]***

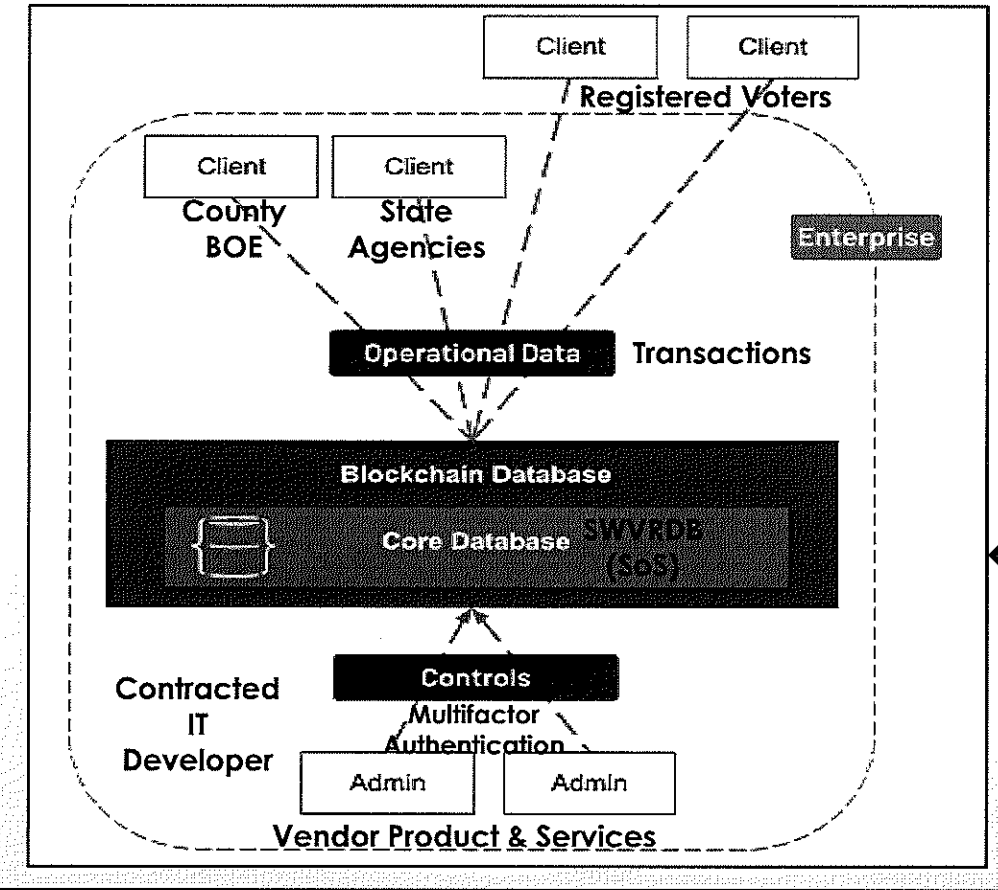
Consortium **ensures no single source owns the data, each validation node has copy of the data *[SoS / State Agencies / Registered Voters***

Operational vs. Non-Operational Data

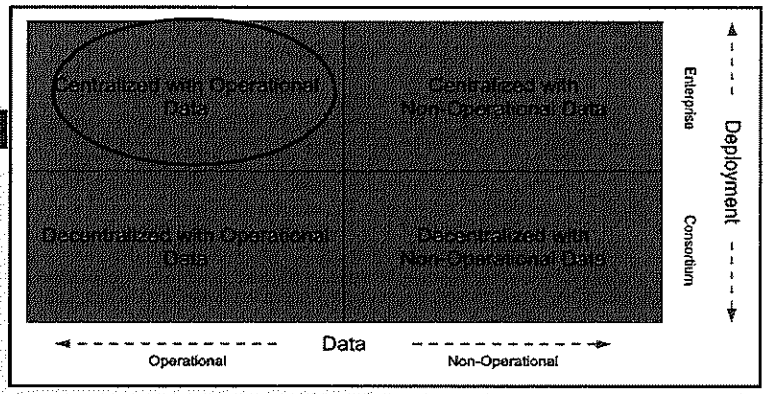
- Data used directly by clients connecting to database is referred to as operational data

Building Blockchain Database Depends on Determining Deployment Scenario and Data Use

Blockchain Use Case – Centralized with Operational Data

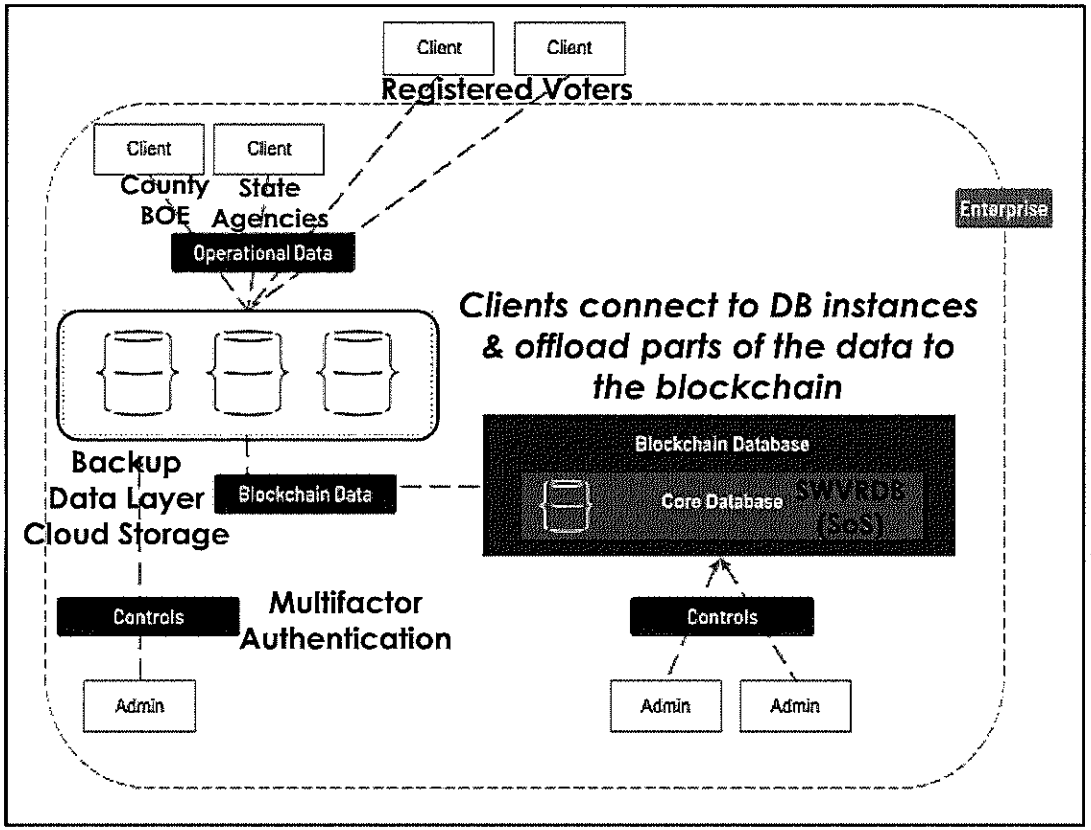


- Deployed within an enterprise ***(SoS/County BOEs)***
- **Provides immutability of documents** created and the **possibility to create and transfer assets**
- Familiar to most developer teams



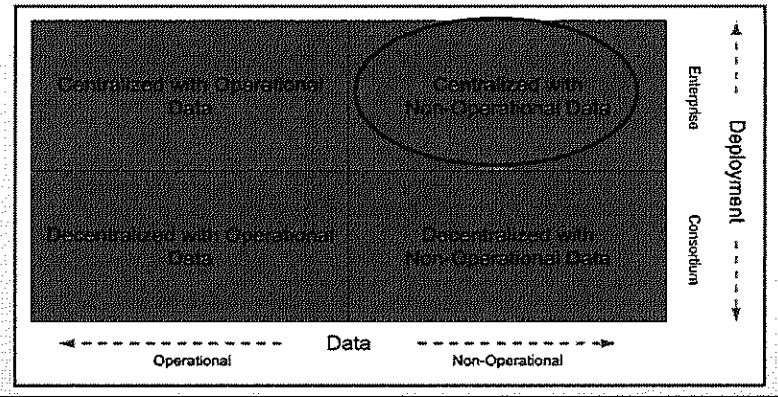
Requires Centralized Mechanism for Authenticating and Authorizing Service and Interface Access

Blockchain Use Case – Centralized with Non-Operational Data



This deployment maintained by a number of administrators *[Current SoS Model for SWVRDB]*

- ***Data is NOT accessed directly by clients*** (i.e. registered voters)
- ***Additional layer reduces the number of nodes*** needed to agree to accept transaction, increasing DB performance
- ***Adds more privacy*** since data is only ***accessible by a limited number of clients*** controlled by enterprise



This Deployment Configuration Embraces Speed and Privacy

Security Model - Authentication and Authorization

Level of Discoverability	Definition
Public	Indicates that anyone can see the dataset record
Protected	Indicates the dataset record will be visible to all but only a subset of fields will be displayed
Private	Only the listed Access Control Groups and Users can see the record (If Private Record is selected, a reason must be provided)

Role	Access Privilege
Reader	The Reader can read records based on permissions
Editor	The Editor can read, create, and edit records based on permissions
Manager	The Manager has Editor access and can delete records and has option to recover or purge datasets
Group Access Control	The user can manage the membership and privileges of other users within access control grp

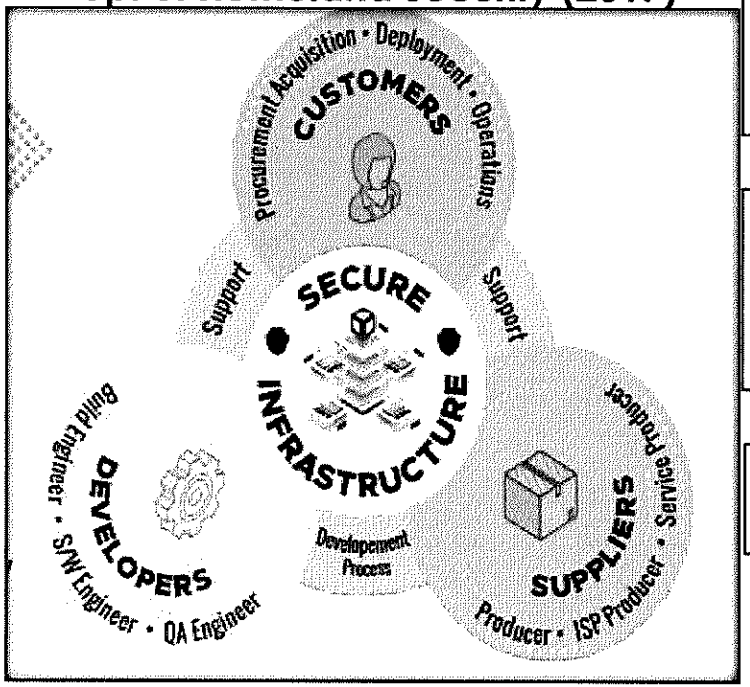
Blockchain is an opportunity to implement:

"States can provide a secure, auditable environment for the processing and exchange of information across entire spectrum of State business"

Blockchain Ledger is opportunity to implement State Identity and Credential Management (SICAM) Guidance

Ohio Voting System Certification – The Solution

Elections are
"National Critical Infrastructure"
-Dept of Homeland Security (2017)

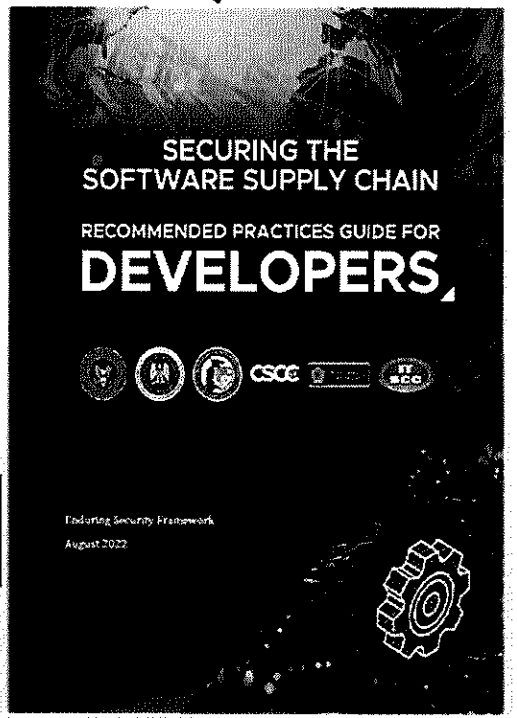


Codify following provisions into law:

1. Adopt Blockchain Digital Ledger Database on top of existing databases

2. Vendors adhere to federal security development practices *and disclose voting system development practices* ***as condition of certification***

3. Introduce in-state 3rd party Independent Cyber Security Reviews



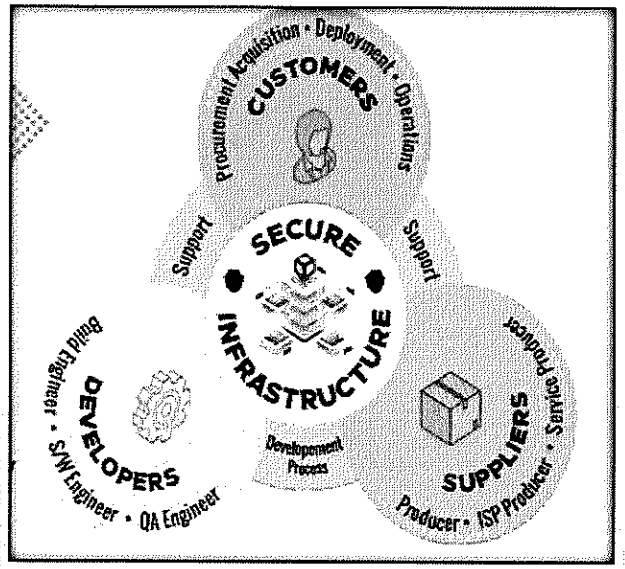
Empower OHIO CYBER RESERVE to lead certification security reviews in partnership with SOS as a pre-requisite to election voting system selection and County BOE procurement

Summary

Challenges

- ***No federal certification standards for most voting systems*** products and services
- Election systems ***continue to certify to obsolete 2005 security standards*** through 2023
- ***No election vendor oversight*** for software supply chain integrity & security development practices
- **Voter registration data is vulnerable and unable to securely track and protect data** from any attack or high privileged user

Recap



Questions?

Solutions

- **Adopt Blockchain Digital Ledger Database** on top of existing relational databases for SoS and Voter Registration supporting Agency Enterprise
- **Vendors shall adhere to federal security development practices**, disclose software byproducts (i.e. artifacts) & agree to 3rd party security review **as condition of certification**
- **Direct Ohio Cyber Reserve to conduct security analysis review** of election vendor systems

Eberhart, Riley

Subject:	Meeting with Dauren Mason to Discuss H.B. 427 Cyber Security Portion
Location:	Microsoft Teams Meeting
Start:	Tue 6/4/2024 10:00 AM
End:	Tue 6/4/2024 10:30 AM
Show Time As:	Tentative
Recurrence:	(none)
Meeting Status:	Not yet responded
Organizer:	Hannum, Logan
Required Attendees:	Willis, Bernard; dauren.h.mason.nfg@army.mil; mstrbic@protonmail.com; Eberhart, Riley
SkypeTeamsProperties:	{"cid":"19:meeting_ZTg5YWM4ZTMtYzhhYy00Y2RlLWJiZGUtMjczNTU0NTc5Yzkw@thread.v2","rid":"0","mid":"0","private":true,"type":0}
SkypeTeamsMeetingUrl:	https://teams.microsoft.com/l/meetup-join/19%3ameeting_ZTg5YWM4ZTMtYzhhYy00Y2RlLWJiZGUtMjczNTU0NTc5Yzkw%40thread.v2/0?context=%7b%22Tid%22%3a%225fbc1338-b4f6-4a8f-91a9-43523a0b679f%22%2c%22Oid%22%3a%226145e2d3-0c79-4374-b47f-385e1650b72a%22%7d
SchedulingServiceUpdateUrl:	https://api.scheduler.teams.microsoft.com/teams/5fbc1338-b4f6-4a8f-91a9-43523a0b679f/6145e2d3-0c79-4374-b47f-385e1650b72a/19_meeting_ZTg5YWM4ZTMtYzhhYy00Y2RlLWJiZGUtMjczNTU0NTc5Yzkw@thread.v2/0
TeamsVtcTenantId:	5fbc1338-b4f6-4a8f-91a9-43523a0b679f
MeetingTemplateId:	default

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 255 398 727 065

Passcode: 3ozsaJ

Dial in by phone

+1 380-215-0572,,308674113# United States, Columbus

Find a local number

Phone conference ID: 308 674 113#

For organizers: Meeting options | Reset dial-in PIN
