



DV^SOrder

Ballot Randomization Flaws Threaten Voter Privacy



Braden L. Crimmins Dhanya Y. Narayanan
J. Alex Halderman
University of Michigan

Drew Springall
Auburn University



AUBURN
UNIVERSITY

The Secret Ballot



Ballot secrecy is a **security mechanism** that prevents bribery and coercion.

Protected by law in all 50 states.

But it is under tension.

Ballot Level Data

Ballot Audit & Review

San Francisco Consolidated Presidential Primary (March 2024) 📄



🖥️ Full Screen

⌵ Filter ballots



🖼️ Front Page

🖼️ Back Page

Official Votes Cast

🖼️ Ballot Audit Log



All

00892_00000_669075

00892_00000_680109

00892_00000_729012

00892_00000_736151

00892_00000_742673

00892_00000_755922

00892_00000_783027

00892_00000_806278

00892_00000_809767

00892_00000_811421

00892_00000_862347

00892_00000_870904

00892_00000_887209

民主黨候選
聯合黨初選
三區市市長, 2024年3月5日

Use a pencil or pen with black or blue ink.
Fill in the oval to the right of your choice, as shown in the picture.
To vote for a qualified write-in candidate, write the candidate's name in the space at the end of the candidate list and fill in the oval.
If you make a mistake, you may request a new ballot.
For information about propositions and opponents of each local ballot measure, refer to your Voter Information Pamphlet starting on page 36 or visit voteinfo.sfelections.org.

請用筆或藍色或黑色的鋼珠筆。
在右方的圓形內填上你的選擇, 如圖所示。
若要投票給符合資格的寫入候選人, 請在候選人名單末尾的圓形內填上候選人的姓名, 並寫明候選人的姓名。
如果你犯錯誤, 你可以要求一張新的選票。
關於每個措施和每個措施的支持與反對者, 請參閱選票(第36頁起)或到 [www.voteinfo.sfelections.org](http://voteinfo.sfelections.org) 查詢。

投票資格和程序: 寫入候選人: 請參閱 (415) 554-4367 或 www.sfelections.org 查詢。
Election rules and procedures: Write-in candidates: See (415) 554-4367 or www.sfelections.org for more information.

This ballot has the presidential control of the party in your voter registration record. To vote a different ballot, contact the Department of Elections at (415) 554-4370 for a replacement ballot.

只有已登記為同一政黨的成員的候選人才能在初選中投票。如需更換選票, 請與選舉局聯繫, 電話: (415) 554-4370。

REGISTRATION / 登記

PRESIDENT OF THE UNITED STATES
美國總統

Presidential Preference
總統候選人

JOSEPH R. BIDEN, JR.
GABRIEL CORNEJO 亞歷克斯·科內霍 / 科內霍
PRESIDENT R. BOODIE 羅曼諾維奇·博迪
JOSEPH R. BIDEN, JR. 約瑟夫·拜登 / 拜登
MARGANNE WILLIAMSON 瑪麗安·威廉森
DEAN PHILLIPS 迪安·菲利普斯

ARMANDO "MANDO" PEREZ-SERRATO 阿曼多·佩雷斯-塞拉托
STEPHEN P. LYONS 史蒂芬·里昂斯
EBAN CAMBRIDGE 伊班·坎布里奇

MEMBER, COUNTY CENTRAL COMMITTEE, ASSEMBLY DISTRICT 19
縣中央委員會成員, 議會選區第19區

PAUL GUSTAFSON 保羅·古斯塔夫森
MARGANNE WILLIAMSON 瑪麗安·威廉森
SUE LEE 蘇·李
LAPRINA HUI 廖麗娜 / 廖麗娜
GREG MARCHAND 格雷格·馬尚
FRANCES HOSH 法蘭絲·荷希
MICHELLE RALSTON 米歇爾·拉爾斯頓
LANCE TUI 蘭斯·圖伊
KEVIN WONG 凱文·黃
SANDRA LEE FEMER 桑德拉·李·費默
CONNIE CHAN 康妮·陳
MICHELE CHEN 米歇爾·陳
QUEENA CHEN 邱金
DAN CALAMACI 丹·卡拉馬奇
LANIER COLES 蘭尼爾·科爾斯
SARA BARZ 薩拉·巴茲
JEN MOSSKOFF 詹·莫斯科夫
CATHERINE STEFANI 凱瑟琳·斯特法尼

Contests

Expand all Collapse all

1. PRESIDENT OF THE UNITED STATES-DEM

- STEPHEN P. LYONS
- EBAN CAMBRIDGE
- GABRIEL CORNEJO
- PRESIDENT R. BOODIE
- JOSEPH R. BIDEN JR.
- MARIANNE WILLIAMSON
- DEAN PHILLIPS
- ARMANDO "MANDO" PEREZ-SERRATO
- Write-in
- WILLIE FELIX CARTER
- PRESIDENT CRISTINA NICOLE GRABO

The DVStorder Vulnerability

DVStorder

DVStorder is a vulnerability that affects data from the **Dominion ImageCast Precinct (ICP/ICP2)** and **ImageCast Evolution (ICE)** ballot scanners.

These are used in 21 states, Puerto Rico, and Canada.

The flaw cannot alter election results.
It can reveal how individuals voted.




The DVSorter Vulnerability

TabulatorNum	BatchId	RecordId	CountingGroup	PrecinctPortion
987	0			
987	0			
987	0			
987	0			
987	0			
987	0			
987	0			
987	0			

```
"Version": "5.10.50.85",  
"ElectionId": "San Francisco 2022 Consolidated General Election",
```

"The ballot images are given a random ID number as their file name, and when the images are extracted by the [EMS] application, they are randomized, thus ensuring the ballot images are de-coupled from voter order"

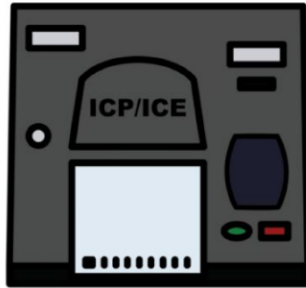
```
idated General EL  
0000_4956870_*.*)"
```

 00210_0000_02503.tif TIF File 70.5 KB	 00210_0000_05799.tif TIF File 116 KB
 00210_0000_040438.tif TIF File 84.5 KB	 00210_0000_041912.tif TIF File 84.0 KB
 00210_0000_040438.tif TIF File 89.1 KB	

- 00893_0000_940512
- 00893_0000_959856
- 00893_0000_984028
- 00893_0000_985107
- 00893_0000_1033020
- 00893_0000_1042676

PRESIDENT OF THE UNITED STATES	
美國總統	
Presidential Preference	
選擇總統候選人	
Vote for One / 選一人	
GABRIEL CORNEJO 加布里埃爾·科爾內霍	ARMANDO "MANDO" PEREZ
PRESIDENT R. BODDIE 普雷西頓特·R·博迪	STEPHEN P. LYONS 史
JOSEPH R. BIDEN JR. 小約瑟夫·R·拜登	EBAN CAMBRIDGE 埃
MARIANNE WILLIAMSON 瑪麗安·威廉森	

Ballot ID Generation



(1) Scanner chooses a random starting point in the cycle



(2) Ballots are assigned subsequent record IDs in order of casting

... 720012 195008 857815 739854 611861 876852 ...

Fixed cycle of 1,000,000 IDs used by all scanners of a given model

The only thing that's "random" is the **starting point** in this list!

Dominion's Obfuscated LCG

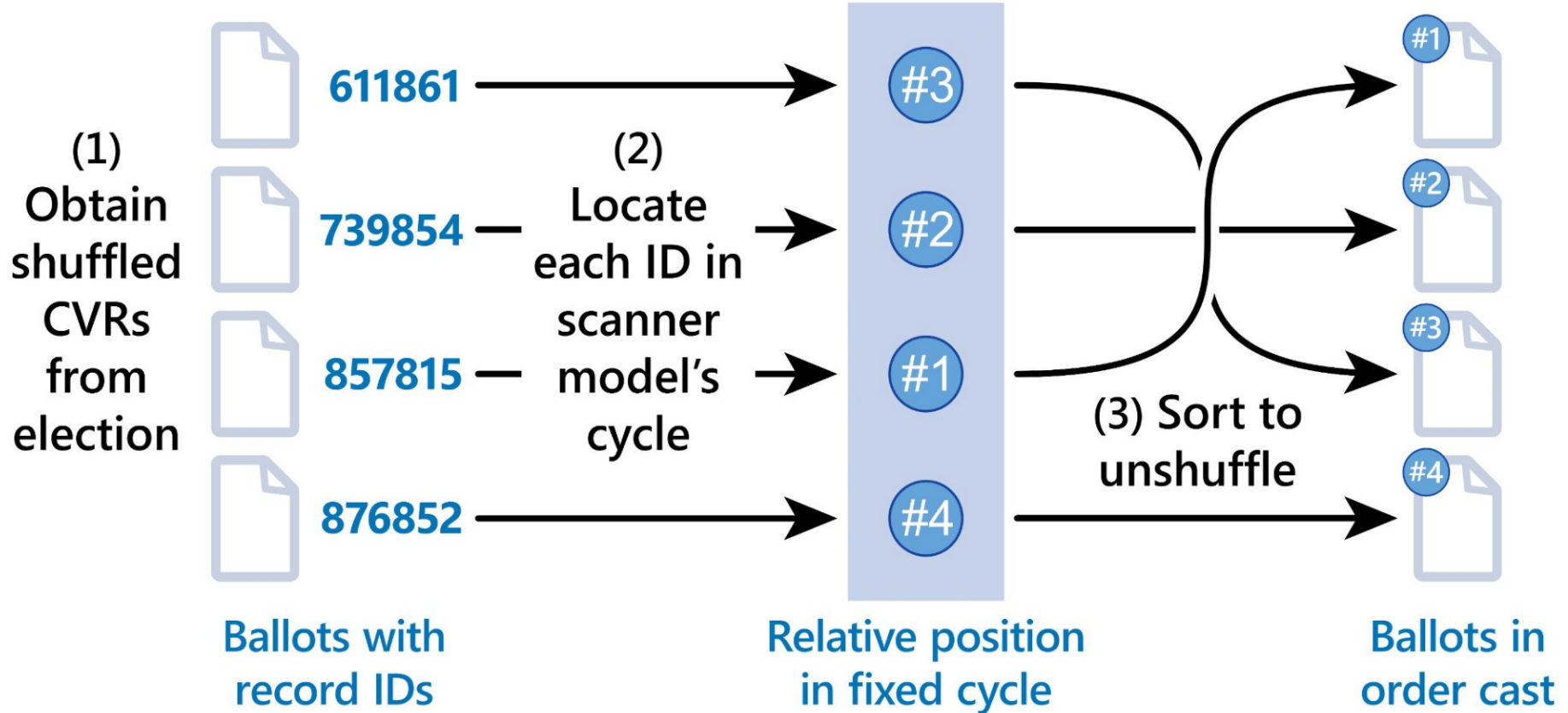
$$x_{n+1} = x_n + 864803 \pmod{1000000}$$

$[0, 1, 2, 3, 4, 5, 6, 7, 8, 9] \longrightarrow [5, 0, 8, 3, 2, 6, 1, 9, 4, 7]$

$123456 \longrightarrow 261534$ $123456 \longrightarrow 342615$

**Check out Section 3 of
our paper!**

Exploiting DVSError to Unshuffle Ballots



Determining Voter Order: (1) On-screen Counter



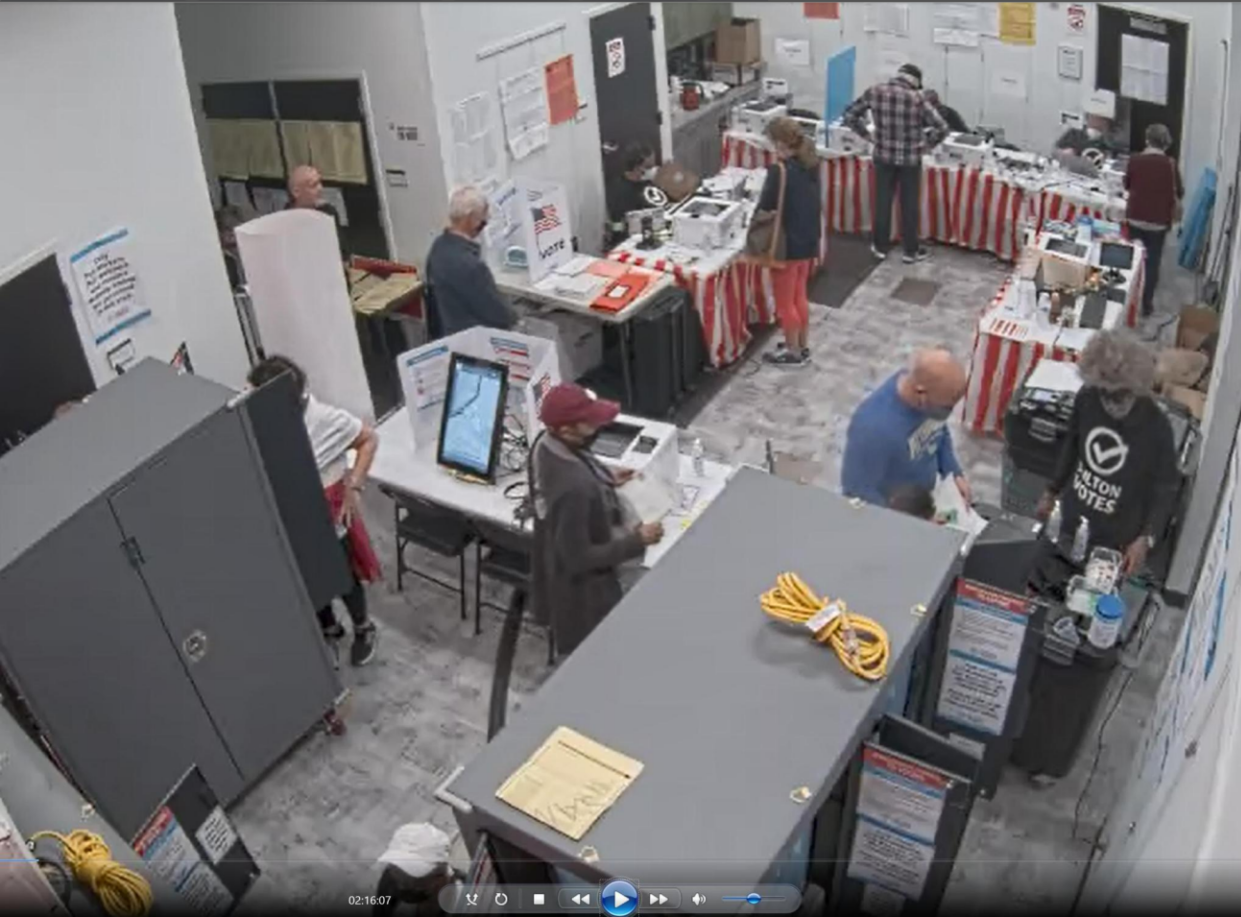
Using the machine's **public counter**, an attacker could learn the index of their victim's ballot.

Determining Voter Order: (2) Watching at the Polls



Partisan observers have a **legal right** to learn voters' identities and monitor as they cast their ballots.

Determining Voter Order: (3) Public Surveillance Video



Some jurisdictions treat **surveillance footage inside polling places** as public record.



DVSSorder

Part 1: The Vulnerability

Part 2: The Aftermath

Highlights election ecosystem security challenges:

1. Coordinated disclosure
2. Prompt and effective mitigation
3. Certification and testing

Election ecosystem security challenges:

1. Coordinated Disclosure

Three Months to the November 2022 Election

July
2022

August

September

October

November

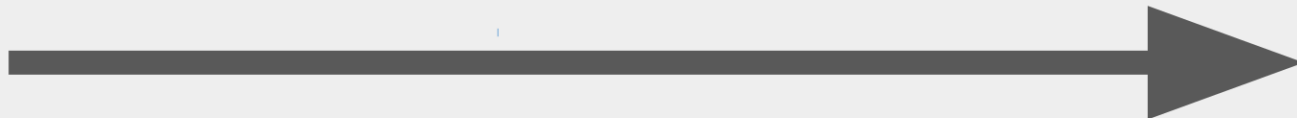
So we found a vulnerability...*now what?*

Options (from least to most onerous)

- ~~Do nothing~~
- Coordinate through Federal entities
- Coordinate through the vendor
- Coordinate directly with the customers

Initial
discovery

Election
Day



CISA's CVD Process

The logo of the Cybersecurity and Infrastructure Security Agency (CISA) is partially visible in the background. It features a blue circular border with the text "SECURITY & INFRASTR" at the top and "SECURITY AGENCY" at the bottom. Inside the circle, there is a stylized blue and white emblem.

Options (from least to most onerous)

- ~~Do nothing~~
- ~~Coordinate through Federal entities~~
- Coordinate through the vendor
- Coordinate directly with the customers

Notifying Dominion

M COLLEGE OF ENGINEERING
COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN
J. Alex Halderman • Professor

August 23, 2022

John Poulos
Dominion Voting Systems
cc: Robert Giles, Nick Ikononakis

Subject: Privacy Flow Affecting Dominion ICP and ICE Tabulators

Dear Mr. Poulos:

We have identified a serious privacy flaw that affects data produced by ImageCast Precinct (ICP) and ImageCast Evolution (ICE) tabulators. Using information that many of your customers make public, such as scan-vote records (CVRs) or ballot images, an attacker can ascertain the order in which all ballots on a machine were cast. In many cases, this would allow attackers to determine how identifiable individuals voted.

Dominion tabulators assign every scanned ballot a record ID number, which, together with tabulator and batch IDs, uniquely identifies each ballot in an election. The record IDs appear in several forms of data produced by the Democracy Suite EMS, including exported CVRs and ballot image filenames, both of which many localities routinely publish or post as public records subject to FOIA. Democracy Suite documentation states that exported CVRs email "to compromise to voter privacy", which implies that the record IDs they contain are intended not to be traceable to specific voters.

However, the method that the ICP and ICE use to generate record IDs is flawed.¹ Each model follows a fixed sequence of one million six-digit numbers. The only parameter that differs from one tabulator or batch to the next is the starting point within the sequence. If an attacker knows the entire sequence, it is a simple matter to determine the order in which all ballots were cast given only the set of record IDs for a batch.²

Using only public information, we were able to deduce the complete record ID sequences for the ICP and ICE and the algorithm that generates them. Rather than a cryptographically secure pseudorandom number generator, each is produced by a linear congruential generator—a kind of algorithm that is vulnerable to a variety of well-known attacks. The output is then reflectively obfuscated by a simple substitution cipher and reordering of digits. The steps we took to deduce the algorithm can potentially be performed using only pen and paper, and there is an appreciable risk that malicious parties will deduce it independently from our work. You can verify that this Python code reproduces the complete record ID sequence for each tabulator:

```
def generate_sequence(p):  
    return [int((15.0 * i + 9.2 * j + 1.1 * A + 71.0 * B) % 1000000 / 100000) + 100000 for i in range(63)  
           for j in range(10000001)]  
seq_sequence = generate_sequence(12, 3, 1, 3, 0, 4)  
seq_sequence = generate_sequence(11, 0, 0, 2, 0, 2)
```

¹<https://www.mitre.org/publications/NotifyingDomination/ICP-DemocracySuite11/Documentation/>
² <https://github.com/0x00sec/ICP-ICE/blob/main/README.md>

All publicly available ICP and ICE ballot images and CVRs that we have examined suffer from this flaw, and it likely affects all current versions of both devices. The ICE tabulator and ICE DRB do not appear to be affected, based on our present knowledge.

Rob and Betty Reyster Building
2260 Hayward Street, Ann Arbor, MI 48109
<https://halderman.com>
jhalderm@umich.edu

and exploited by members of the public without
to some examples of circumstances where an attacker



ing CVRs and ballot images, is an important form of
For this reason, it is imperative to provide solutions
to, both for upcoming elections and for those in the
without further loss of transparency by appropriately
documenting the process outlined below.

generate key unique to the election, tabulator, and batch,
unique, cryptographically strong permutation.
age filenames with the encrypted values.
position times), and sent CVR entries and image files.
ation is removed.

to accomplish these steps.

State the ICP and ICE software to replace the record
would be happy to provide advice concerning such a



ICP or ICE about this problem before the November
inmutable data. For this reason, we plan to publicly
ize. We will also inform appropriate federal agencies
liberal jurisdictions that we know have published
an opportunity to sanitize it.
and we would be happy to collaborate in efforts to
fix this problem.

Rob and Betty Reyster Building
2260 Hayward Street, Ann Arbor, MI 48109
<https://halderman.com>
jhalderm@umich.edu

ing CVRs and ballot images, is an important form of
For this reason, it is imperative to provide solutions
to, both for upcoming elections and for those in the
without further loss of transparency by appropriately
documenting the process outlined below.

generate key unique to the election, tabulator, and batch,
unique, cryptographically strong permutation.
age filenames with the encrypted values.
position times), and sent CVR entries and image files.
ation is removed.

to accomplish these steps.

State the ICP and ICE software to replace the record
would be happy to provide advice concerning such a

ICP or ICE about this problem before the November
inmutable data. For this reason, we plan to publicly
ize. We will also inform appropriate federal agencies
liberal jurisdictions that we know have published
an opportunity to sanitize it.
and we would be happy to collaborate in efforts to
fix this problem.

Staden L. Crimmins
Graduate Student Research Assistant
Computer Science & Engineering

Rob and Betty Reyster Building
2260 Hayward Street, Ann Arbor, MI 48109
<https://halderman.com>
jhalderm@umich.edu

August 2022: Personally called Dominion CEO and sent detailed written notification

- Code to generate RNG sequences
- Descriptions of threat scenarios
- Recommended mitigations

We set deadline ahead of Nov. election for public disclosure.

Offered to collaborate with them and assist in solving the issue.

Dominion's Customer Notification



September 9, 2022

Customer Notification: Cast Vote Selections

Dominion is aware that many customers are receiving requests to provide access to election records or results reports which identify cast vote selections. While definitions and requirements can vary widely, this general guidance is designed to help support customers in identifying the best way to respond to such requests, in consultation with your legal advisors.

It is important to follow any state or local requirements guiding public access to and release of cast vote records ("CVRs"), including paper ballots or ballot images.

As a best practice, CVR data that is being released for public inspection should follow state and local laws to preserve voter secrecy. Customers should consult their legal advisors for guidance on how best to ensure such protections are applied, particularly if simultaneously releasing any record (ie. video) that could reveal a voter's identity in the order in which they cast their ballot.

MORE: [National Institute of Standards & Technology \("NIST"\): Cast Vote Records Common Data Format Specification \(2019\)](#)

Problems:

- **Doesn't mention there's a vulnerability!**
- Suggests customers "follow state and local laws" when releasing ballot data.
- But... customers left to rely on Dominion's previous, inaccurate assurance that ballots are safely shuffled.

(Didn't tell us they sent this.
We found out weeks later.)

This is the *entire advisory*.

Dominion's Updated Customer Advisory

*UPDATE: A researcher who has been granted extensive access to the Dominion 5.5A system has claimed to have a method by which to reveal how Democracy Suite scrambles Cast Vote images as they are saved. **Following the information described in this advisory mitigates any potential risk that may result as part of any such disclosure.** For customers using platforms other than a 5.5 device, we advise the following options to mitigate risk. We cannot guarantee mitigation with any quality of service. We do not have any control over the security of the device. We do not have control over the device's network connection. We do not have control over the device's software. We do not have control over the device's hardware. We do not have control over the device's firmware. We do not have control over the device's configuration. We do not have control over the device's data. We do not have control over the device's logs. We do not have control over the device's updates. We do not have control over the device's security. We do not have control over the device's privacy. We do not have control over the device's performance. We do not have control over the device's reliability. We do not have control over the device's availability. We do not have control over the device's integrity. We do not have control over the device's confidentiality. We do not have control over the device's authenticity. We do not have control over the device's accountability. We do not have control over the device's transparency. We do not have control over the device's openness. We do not have control over the device's inclusivity. We do not have control over the device's diversity. We do not have control over the device's equity. We do not have control over the device's justice. We do not have control over the device's freedom. We do not have control over the device's democracy. We do not have control over the device's human rights. We do not have control over the device's rule of law. We do not have control over the device's accountability. We do not have control over the device's transparency. We do not have control over the device's openness. We do not have control over the device's inclusivity. We do not have control over the device's diversity. We do not have control over the device's equity. We do not have control over the device's justice. We do not have control over the device's freedom. We do not have control over the device's democracy. We do not have control over the device's human rights. We do not have control over the device's rule of law.*

Options (from least to most onerous)

- ~~• Do nothing~~
- ~~• Coordinate through Federal entities~~
- ~~• Coordinate through the vendor~~
- Coordinate directly with the customers

This is the *only*

Finally, m

(1) Falsely im

5.5-series devices — *even after Dominion had a month to commit findings!*

(2) Misleadingly states that “following the information described in this advisory mitigates any potential risk” — *but there is no mitigation information!*

n't talk to us.

But...

y affect

How Best to Contact Election Officials?

<name>,

I think you offered to provide some appropriate contacts at the state level too. If that's still on offer, we could use those for jurisdictions that use the affected equipment.

Thanks,
Alex

On Wed, Sep 7, 2022, 6:51 PM [REDACTED] <[REDACTED]@cisa.dhs.gov> wrote:

I don't have those handy right now but I can ask the ESI team (Geoff Hale and company). Let me see what we can do.

<signature block>

[REDACTED] <[REDACTED]@cisa.dhs.gov>

Sep 19, 2022, 1:22 PM

to me ▾
My apologies, but we apparently must direct you to [Our Members — NASED](#) rather than drilling down into who runs what exactly. Sorry for the delay.

Google every state election director contact X [voice search] [image search] [search]

All News Images Videos Books More Tools

About 1,380,000,000 results (0.29 seconds)

Federal Election Commission (.gov)
<https://www.fec.gov/introduction-campaign-finance>

How To Research Public Records|State Election Offices - FEC

State	Office	Website
American Samoa	Election Office, Pago Pago, AS	https://aselectionoffice.gov
District of Columbia	Board of Elections, Washington, DC	https://www.dcboe.org/
Guam	Guam Election Commission, Hagatna, GU	http://gec.guam.gov/

View 55 more rows

Alabama.gov
<https://www.sos.alabama.gov/alabama-votes/voter>

Absentee Voting Information | Alabama Secretary of State

Absentee ballot applications delivered by mail must be received in the office of the Absentee Election Manager for your county no later than 7 days prior to ...

<https://www.sos.alabama.gov/alabama-votes/board...>

Board of Registrars: All Counties - Alabama Secretary of State

Board of Registrars: All Counties. County, Email, Mailing Address, Physical Address, Phone, Autauga, Autauga@vote.alabama.gov, P.O. Box 680036,

NASED
<https://www.nased.org>

National Association of State Election Directors (NASED)

In each of their states, they are responsible for implementing election laws and policies, maintaining the voter registration databases, working with local ...

Example: San Francisco

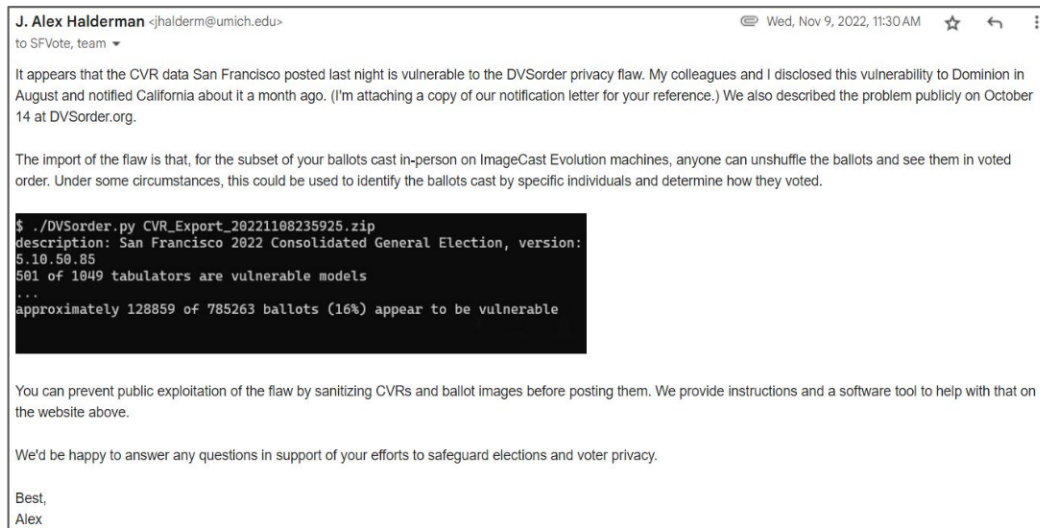
San Francisco is a leader in transparency and **routinely publishes ballot-level data**.
We named them specifically in our disclosures to Dominion and CA.

Apparently, nobody warned San Francisco it was vulnerable!

SF began publishing new vulnerable data on Nov. 8, 2022.

SF officials say they never heard from the state and couldn't understand Dominion's advisory.

In 2024, SF tried but failed to sanitize the data they posted. They removed only one of several appearances of the vulnerable IDs in the records.



Example: San Francisco

San Francisco is a leader in transparency and **routinely publishes ballot-level data**.
We named them specifically in our disclosures to Dominion and CA.

Apparently, nobody warned San Francisco it was vulnerable!

SF began publishing new vulnerable data on Nov. 8, 2022.

SF officials say they never heard from the state and couldn't understand Dominion's advisory.

In 2024, SF tried but failed to sanitize the data they posted. They removed only one of several appearances of the vulnerable IDs in the records.

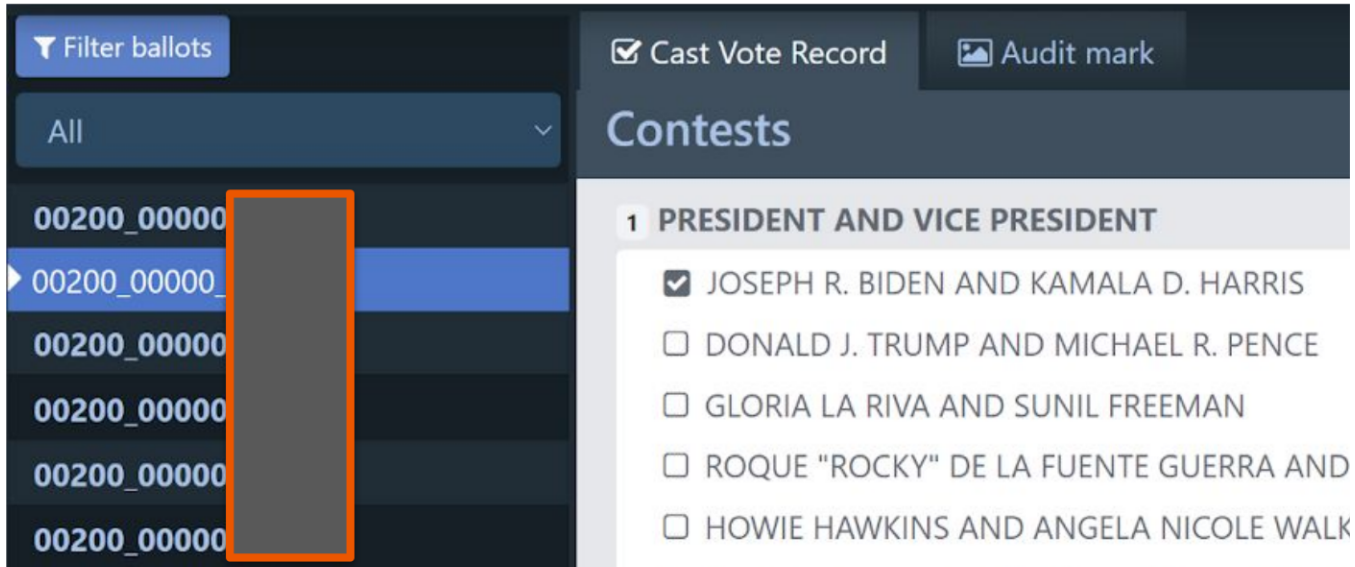
Recommendations:

- Vendors should accept responsibility and convey accurate vulnerability information
- The federal government should reliably coordinate disclosure for vulnerabilities in election infrastructure

Election ecosystem security challenges:

2. Effective Mitigation

Effective Mitigation



The screenshot displays a user interface for casting a vote. On the left, a list of ballot IDs (00200_00000) is shown, with one ID highlighted in blue. A vertical grey bar with an orange border obscures the names of the candidates for the selected ballot. On the right, the 'Contests' section is visible, showing a list of candidates for the 'PRESIDENT AND VICE PRESIDENT' contest. The first candidate, 'JOSEPH R. BIDEN AND KAMALA D. HARRIS', is selected with a checked checkbox. Other candidates include 'DONALD J. TRUMP AND MICHAEL R. PENCE', 'GLORIA LA RIVA AND SUNIL FREEMAN', 'ROQUE "ROCKY" DE LA FUENTE GUERRA AND', and 'HOWIE HAWKINS AND ANGELA NICOLE WALK'. The interface also includes a 'Filter ballots' button, a 'Cast Vote Record' checkbox, and an 'Audit mark' button.

The immediate mitigation is to remove or replace the ballot IDs and reshuffle before publishing data.

Our Automated Sanitizer Tool

We created **open-source tool** to help officials reprocess ballot-level data so that DVSorder can't be exploited by the public. Available from **DVSorder.org**.

To sanitize a single CSV-format CVR file

```
dvsanitizer --gen-seed --sanitize-csv --input dirty-data/CVR_Export_1234.csv --output-dir clean-data/
```

Sanitize a single JSON-format CVR .zip file:

```
dvsanitizer --gen-seed --sanitize-json-zip --input dirty-data/CVR_Export_1234.zip --output-dir clean-data/
```

To sanitize a folder (or folder hierarchy) of .tif ballot images:

```
dvsanitizer --gen-seed --sanitize-tif-dir --input dirty-data/ballot-images/ --output-dir clean-data/ballo
```

Dominion Software Update (D-Suite 5.17)

PRO V&V



6705 Odyssey Drive
Suite C
Huntsville, AL 35806
Phone (256)713-1111
Fax (256)713-1112

Test Plan for EAC 2005 VVSG Certification Testing
Dominion Voting Systems Democracy Suite (D-Suite) Version 5.17
Voting System

General System Changes

- Improved pseudo random number algorithm

Dominion incorporated its patch into a major update, necessitating a **lengthy federal review**.

Delayed availability until almost **5 months after public disclosure**.

Recommendation:

Produce discrete security patches that can be rapidly certified.

Example: Georgia – Still vulnerable two years later

The entire state of Georgia uses tabulators vulnerable to DVSSorder.
Georgia counties continue to publish vulnerable data in 2024.

Georgia announced in May 2023 that it won't patch until after 2024 presidential election.

Recommendation:

States should patch at a regular cadence and be prepared for emergency updates as needed.



The screenshot shows the top portion of a press release from the Georgia Secretary of State's office. The header includes the state seal, the name of the Secretary of State Brad Raffensperger, and navigation links for various departments. The main title of the press release is "Georgia Secretary of State Brad Raffensperger Continues Focus on Security in Preparation for 2024 Elections", dated May 19th, 2023. The text of the press release states that the Elections Division announced plans for security preparations for the upcoming Presidential Election Year.

Georgia
Secretary of State
Brad Raffensperger

SOS Office ▾ Business ▾ Charities ▾ Elections ▾ Securities ▾

Georgia Secretary of State Brad Raffensperger Continues Focus on Security in Preparation for 2024 Elections

May 19th, 2023

Atlanta – Georgia Secretary of State Brad Raffensperger's Elections Division announced on a call with county election officials the plan and timeline of security preparations for the upcoming Presidential Election Year.

Also, in reviewing the processes it will require an update of the nearly 45,000 pieces of voting equipment, along with the subsequent acceptance testing. This process will take tens of thousands of man hours. **Therefore, the statewide move to 5.17 will occur following the 2024 election cycle.** This will allow the state and counties to focus on executing municipal elections and running the Presidential cycle. It also allows the state to put together a thoughtful, thorough plan to roll out the latest software.

Election ecosystem security challenges:

3. Certification and Testing

Two Decades of Voting Machine Randomness Failures

Experts have been pointing out **for 20 years** that broken random number generation threatens voter privacy. **Public availability of ballot-level data has brought this issue to a head.**

Diebold AccuVote TS

Kohno et al. (2003)

Used an LCG with a predictable seed

Sequoia AVC Edge

Blaze et al. (2007)

Only 10 possible random sequences

Hart InterCivic machines

Inguva et al. (2007)

Used a poorly randomized data structure

Diebold DREs in Brazil

Aranha et al. (2014)

Used C's rand function, seeded with the time in seconds the system turned on

Gaps in Federal and State Certification



Federal and state governments require testing and certification for election equipment

Vulnerable Dominion scanners passed testing or certification *at least a dozen times*

Certification requirements lack detailed coverage of privacy

Recommendation:

Rigorously test for privacy problems, drawing on lessons from past vulnerabilities

DVOrder: A Wake-Up Call for Voter Privacy

DVOrder should be a wake-up call that election sector needs to take voter privacy more seriously.

- How is it possible that in 2022, a leading voting system vendor thought shuffling ballots with an LCG was appropriate?
- Why didn't this raise red flags with regulators during any one of their dozen certification reviews?
- Why can't jurisdictions as large as Georgia or as sophisticated as San Francisco address the problem even years after they learned about it?

If the right to a secret ballot is to mean anything, actors across the election technology space must do their part to protect it.



DV^SOrder

Ballot Randomization Flaws Threaten Voter Privacy



Braden L. Crimmins Dhanya Y. Narayanan
J. Alex Halderman
University of Michigan

Drew Springall
Auburn University



AUBURN
UNIVERSITY