Elections and Cybersecurity
What Could Go Wrong?

Lecture slides by J. Alex Halderman
University of Michigan

What **Security Requirements** do election systems need to enforce?

Integrity

The outcome matches voter intent.

Votes are counted as cast (outcome).

Votes are cast as intended (intent).

Security Requirements

☑ Integrity

Ballot Secrecy

Weak form:

Nobody can figure out how you voted…

Strong form:

…even if you try to prove it to them.

Security Requirements

- ☑ Integrity
- ☑ Ballot Secrecy

Voter Authentication

Only authorized voters can cast votes,

and

each voter can only vote up to the permitted number of times.

Security Requirements

- ☑ Integrity
- ☑ Ballot Secrecy
- ☑ Voter Authentication

Enfranchisement

All authorized voters have the opportunity to vote.

Security Requirements

- ☑ Integrity
- ☑ Ballot Secrecy
- ☑ Voter Authentication
- ☑ Enfranchisement

Availability

The election system is able to accept all votes on schedule and produce results in a timely manner.

Security Requirements

- ☑ Integrity
- ☑ Ballot Secrecy
- ☑ Voter Authentication
- ☑ Enfranchisement
- ☑ Availability

Voting as a Security Problem?

Plus…No Universally Trusted Parties

Voting Technology

Voice Voting

The County Election
(Missouri, c.1846)
George Caleb Bingham
1851-2

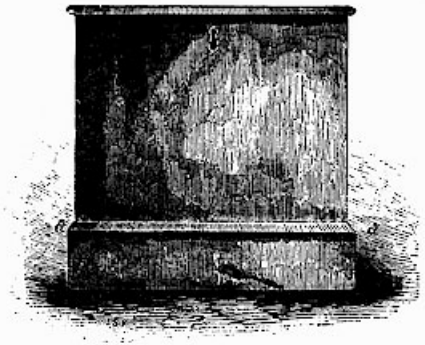
Voice Voting

Voice Voting…
What could go wrong?!?

Voice Voting…
What could go wrong?!?

Wooden Ballot Box

U.S., c.1870

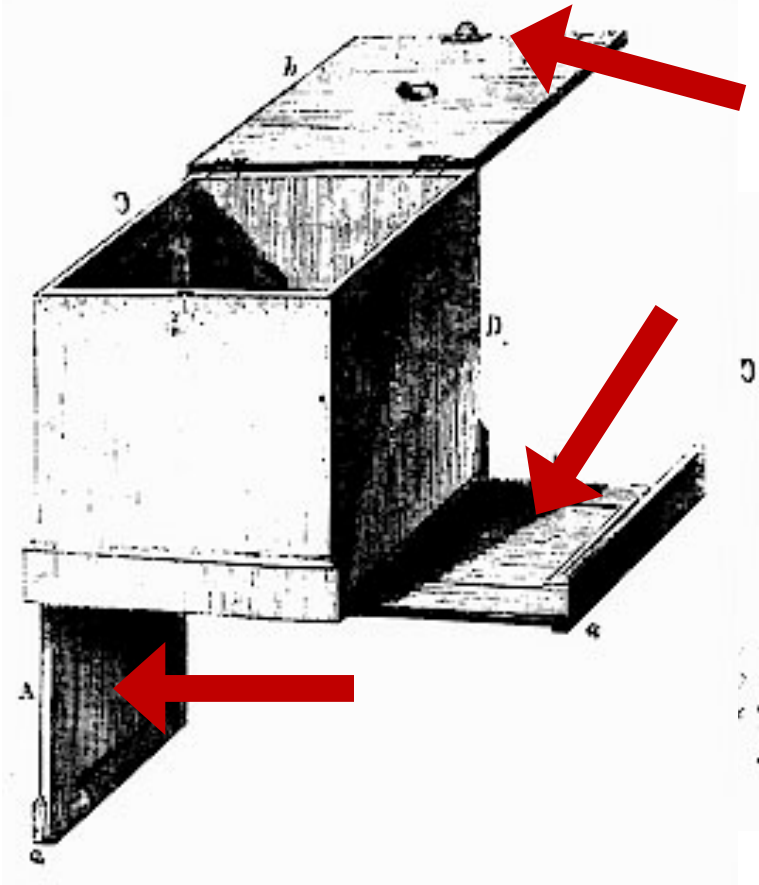


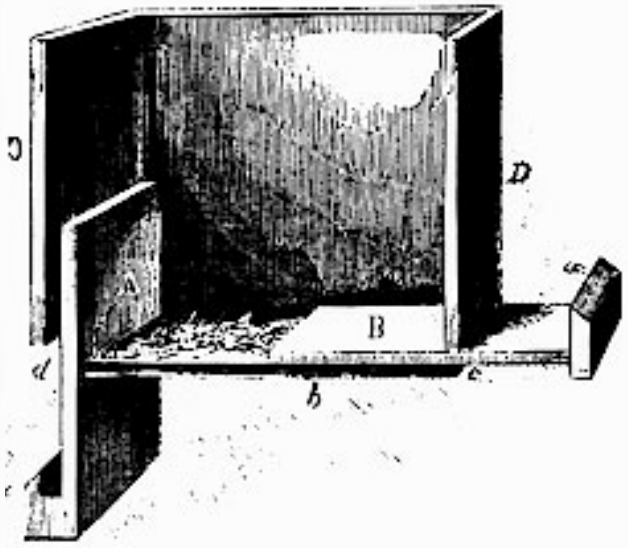
THE STUFFER'S BALLOT-BOX CLOSED UP.

STUFFER'S BALLOT-BOX.

WE give three views of the "Stuffer's Ballot-Box," which will give the reader a clear idea of the *modus operandi* of conducting the elections in San Francisco, and probably in some of our northern cities. The drawings were made from the box now in possession of the Vigilance Committee. It was from ballots taken from this box that Yankee Sullivan made out the election returns that secured Casey his office of Supervisor. The box is about two feet long and fourteen inches wide, and a foot deep, and painted on the outside a dark sky-blue color. It had moulding or cleats around the bottom, and at the top next the lid. The lock, which looked like an ordinary one, is so constructed that though it is worked with a key, it might also be opened by a peculiar pressure upon one side of the lid. There was an auger hole in the middle of the lid, and some of the wax with which it had been sealed at the closing of the polls when last used, was still remaining. It seems that the box was used last at a primary election in the Seventh ward, and the votes were still in it. On looking at the ballot-box, few would suspect the contrivances about it; but on further and minute examination it was found that it had a false bottom and a false side, sliding in grooves, under and behind which were packed quantities of spurious votes all ready for an election.

The mode of working the machine seems to have been this: A sufficient number of the votes which the initiated wished to elect, were prepared and secreted under and behind the false bottom and side. The election was held: Smith was the man to be elected, but Brown was the man of the people's choice. The polls were then closed, and the box sealed and placed in the hands of some one in the secret. The stuffer then drew out the false bottom at his convenience, turned the box upside down, shoved the bottom back and Smith had a majority of the votes: or suppose Brown had still a majority, the false side was pulled down, and another reservoir of votes for Smith was opened. Smith now had a triumphant majority, though the seal had not been touched; or if nothing else would do, a handful of votes for Smith might be easily thrown in, and in each case the lid would probably be opened, and polled votes corresponding with the number of the stuffed ones be withdrawn. One thing was certain—Smith would be elected.





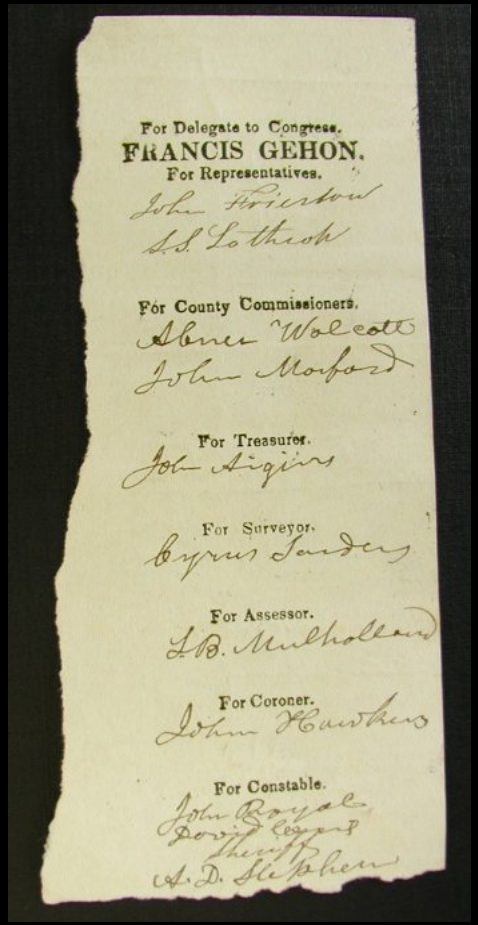
THE STUFFER'S BALLOT-BOX—INTERIOR VIEW.

Glass Ballot Box

U.S., 1884

Acme Voting Machine

U.S., c.1880


For Delegate to Congress.
FRANCIS GEHON.
For Representatives.
John Frierson
A. S. Lathrop

For County Commissioners.
Abner Wolcott
John Morford

For Treasurer.
John Aigins

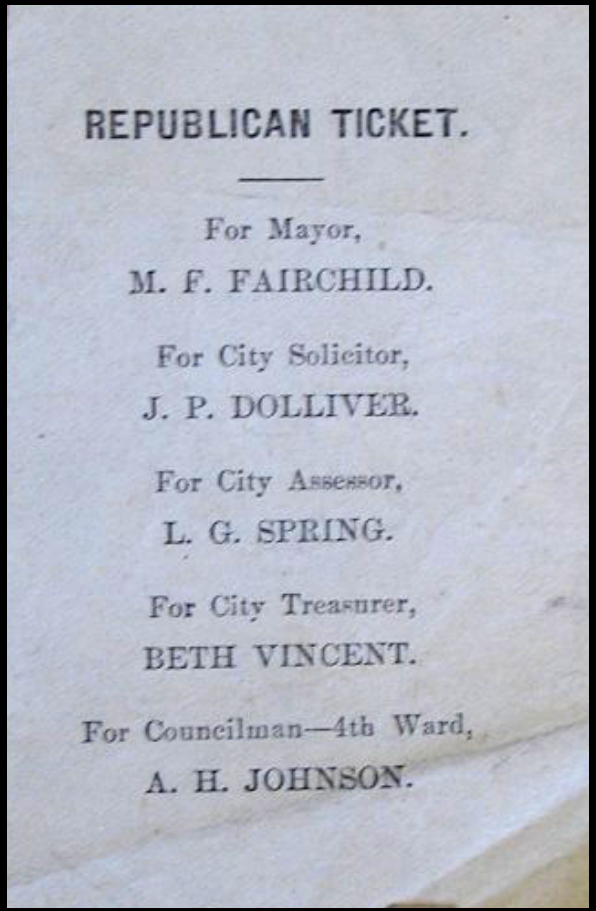
For Surveyor.
Cyrus Sanders

For Assessor.
L. B. Mulholland

For Coroner.
John Hawkins

For Constable.
John Royal
David Logan
Sheriff
A. D. Stephens

1839


REPUBLICAN TICKET.

For Mayor,
M. F. FAIRCHILD.

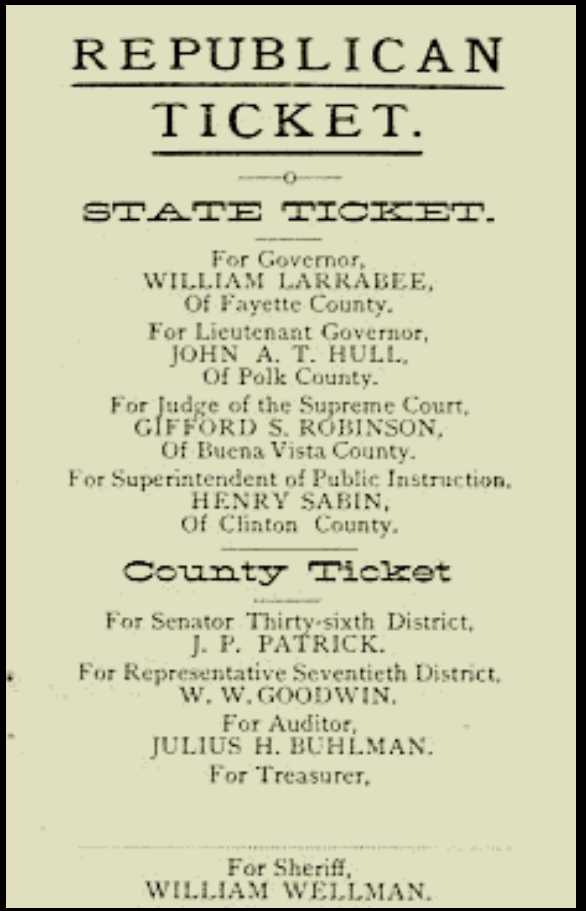
For City Solicitor,
J. P. DOLLIVER.

For City Assessor,
L. G. SPRING.

For City Treasurer,
BETH VINCENT.

For Councilman—4th Ward,
A. H. JOHNSON.

1880


REPUBLICAN
TICKET.

STATE TICKET.

For Governor,
WILLIAM LARRABEE,
Of Fayette County.
For Lieutenant Governor,
JOHN A. T. HULL,
Of Polk County.
For Judge of the Supreme Court,
GIFFORD S. ROBINSON,
Of Buena Vista County.
For Superintendent of Public Instruction,
HENRY SABIN,
Of Clinton County.

County Ticket

For Senator Thirty-sixth District,
J. P. PATRICK.
For Representative Seventieth District,
W. W. GOODWIN.
For Auditor,
JULIUS H. BUHLMAN.
For Treasurer,

For Sheriff,
WILLIAM WELLMAN.

1888

Democratic Primary Election
RICHLAND COUNTY

September 12, 1916

For House of Representatives.
(Vote for four, scratch others.)

F. WM. CAPPELMANN.
JOHN W. CREWS.
~~W. D. HAMPTON.~~
JAS. A. HOYT.
M. C. LUMPKIN.
~~J. T. MILLER.~~
J. M. RAWLINSON.
R. H. WELCH.

For Sheriff.
(Vote for One, Scratch other.)

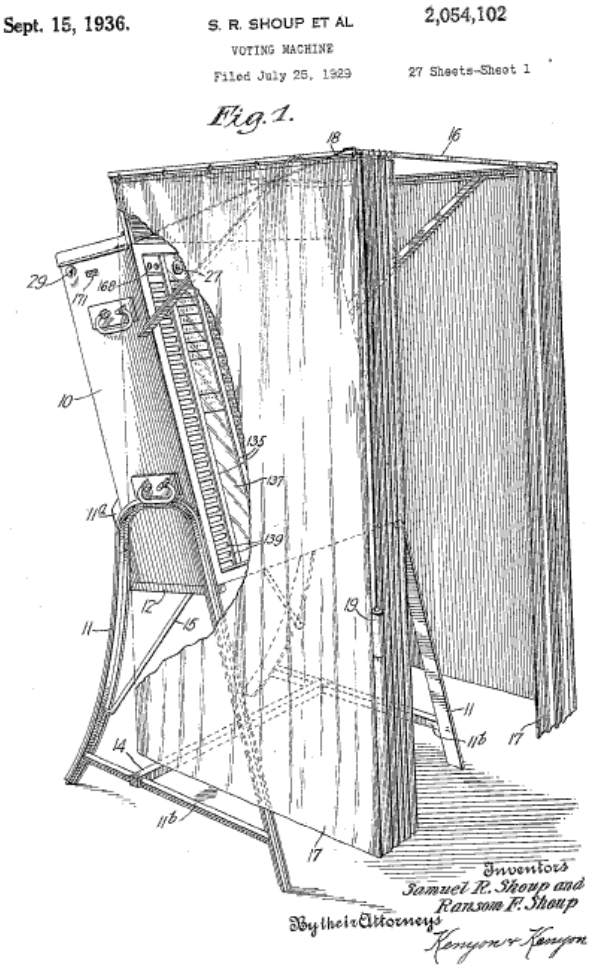
~~J. C. McCAIN.~~
GEO. W. TAYLOR.

For Coroner.
(Vote for One, Scratch other.)

~~W. J. JONES.~~
J. A. SCOTT.

1893

DEMOCRATIC.	REPUBLICAN.
	Majorities
FOR MAYOR, AUGUST LEUZ, JR. CORNER BURLINGTON AND JOHNSON STREETS.	FOR MAYOR, CHAS. LEWIS 221 NO. 227 NORTH CLINTON STREET.
FOR TREASURER, GEORGE W. KOONTZ 848 NO. 620 EAST BURLINGTON STREET.	FOR TREASURER,
FOR CITY SOLICITOR, FRANK J. HORAK NO. 120 DODGE STREET.	FOR SOLICITOR, L. H. FULLER 101 NO. 422 SOUTH DUBUQUE STREET.
FOR ASSESSOR, F. A. HEINSIUS NO. 948 EAST MARKET STREET.	FOR ASSESSOR, H. W. LATHROP 198 NO. 518 IOWA AVENUE.
FOURTH WARD.	FOURTH WARD.
FOR TRUSTEE, JOHN U. MILLER 24 EAST MARKET STREET.	FOR TRUSTEE, J. C. LEASURE COR. VAN BUREN ST. AND IOWA AVENUE.


Sept. 15, 1936. S. R. SHOUP ET AL 2,054,102

VOTING MACHINE

Filed July 25, 1929 27 Sheets-Sheet 1

Fig. 1.

Inventors
Samuel R. Shoup and
Ransom F. Shoup
By their Attorneys
Kenyon & Kenyon

Voting Machine Patent

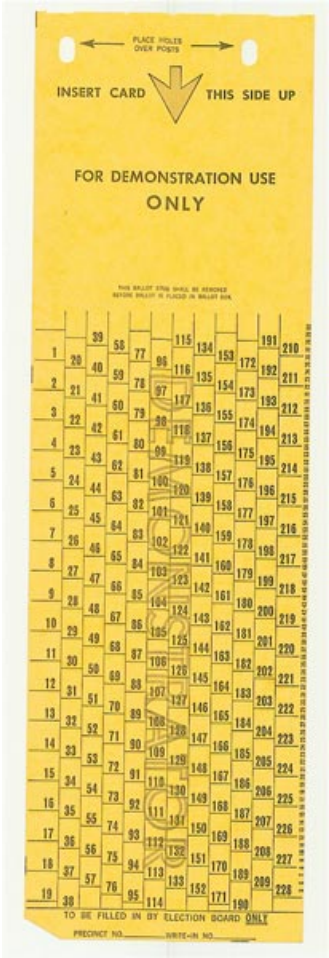
1936

Voting Machine

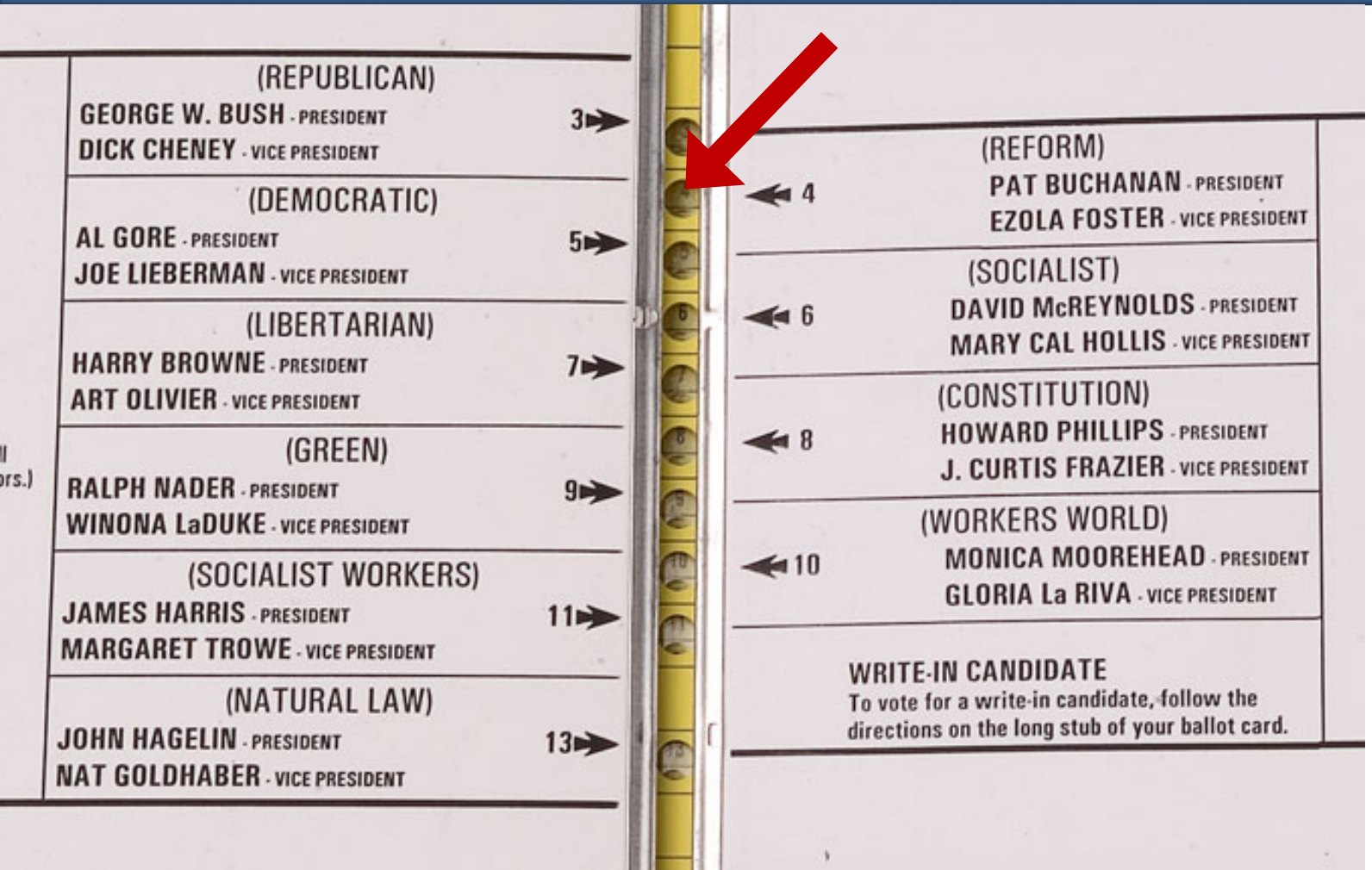
1890s

Votomatic Vote Recorder

1964

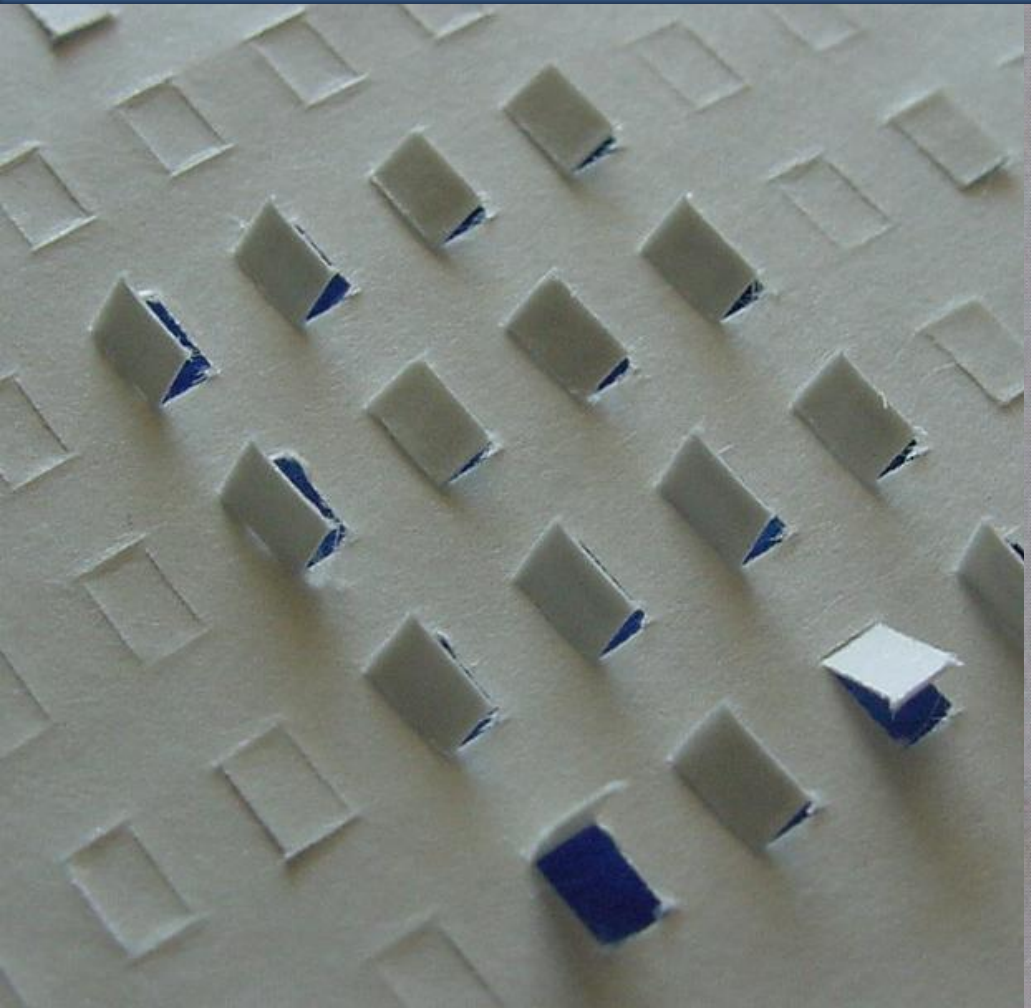


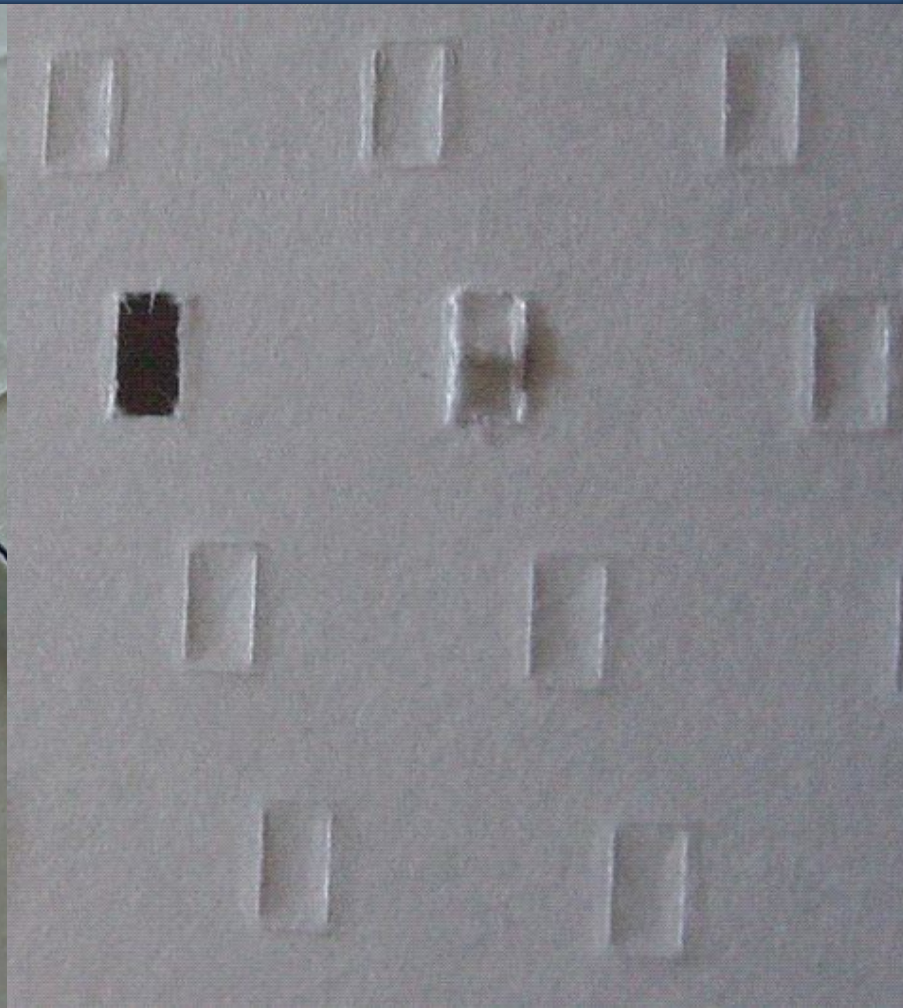
Votomatic Punch Card



Votomatic Butterfly Ballot

Florida, 2000



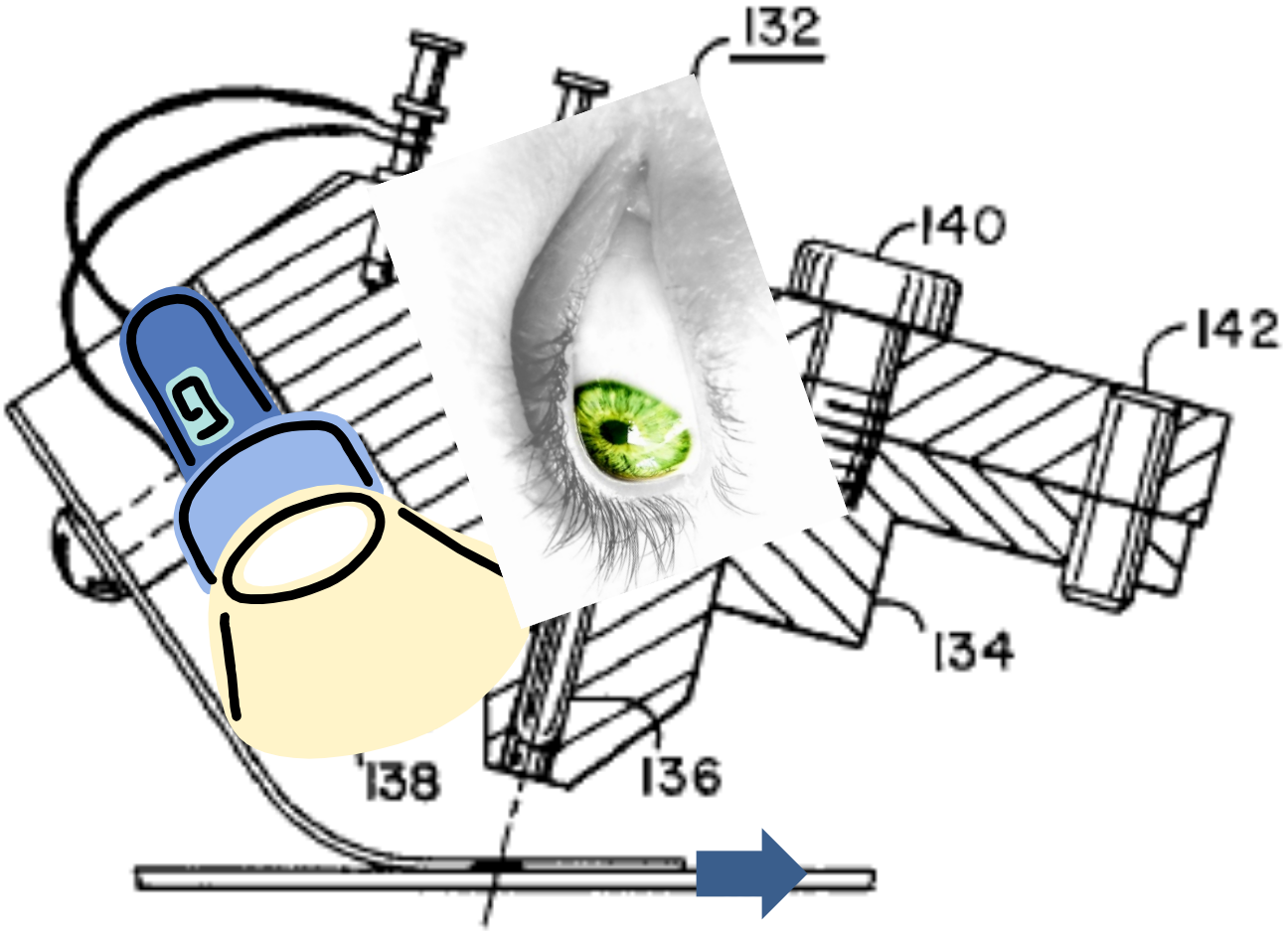


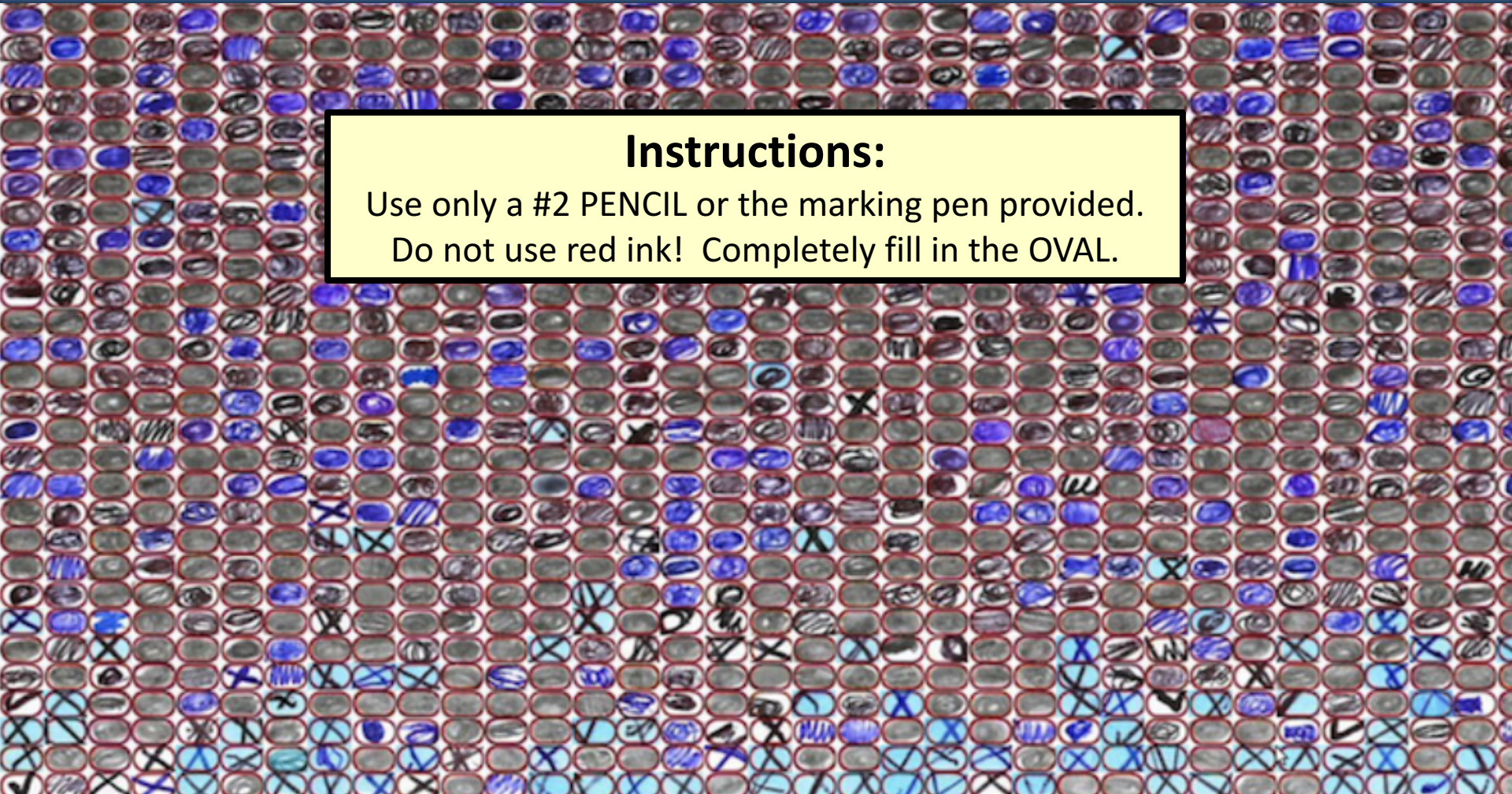
Computers at the Polls

DREs **Optical Scan** = **Computers**


FIFTH
DISTRICT
3


Memory Card
OPTECH III-P
Eagle
INSERT BALLOT HERE
1
2

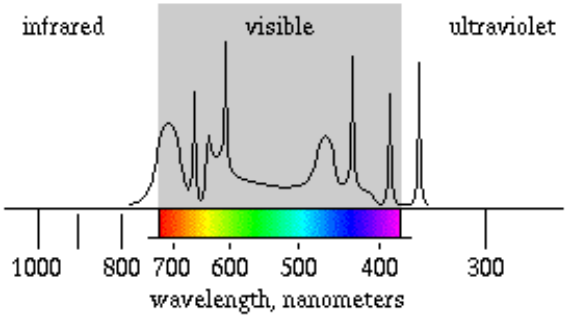

132
140
142
134
138
136

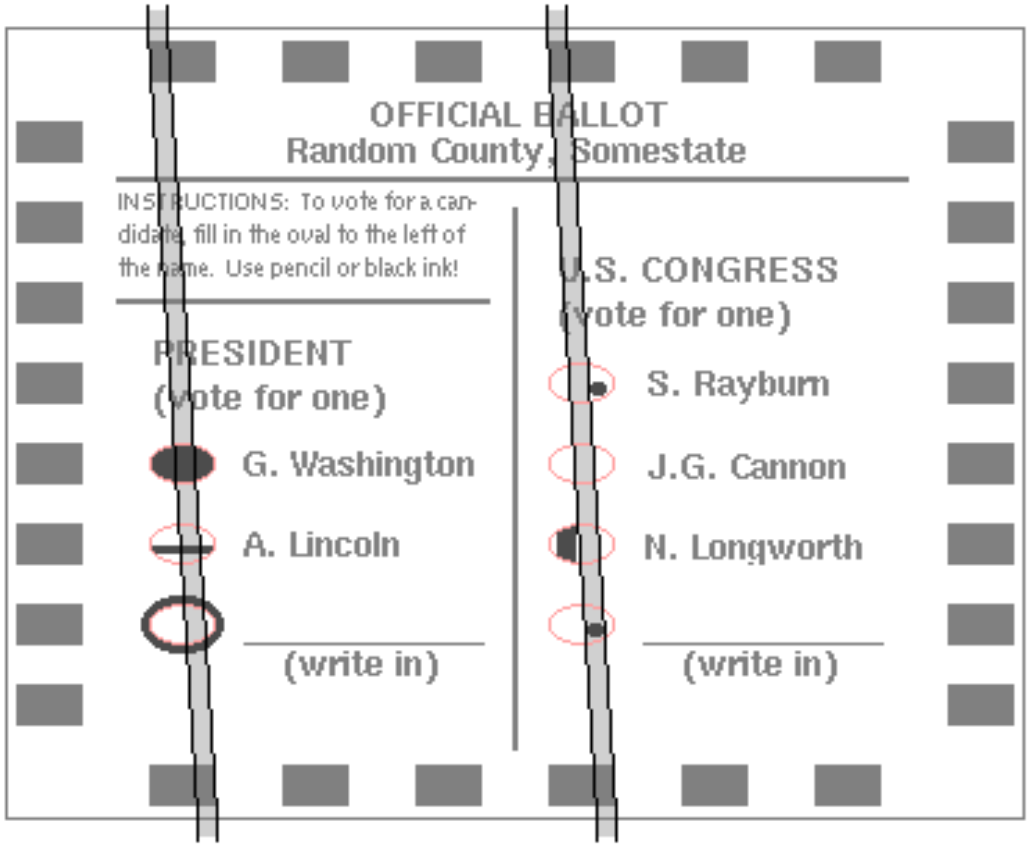


Instructions:

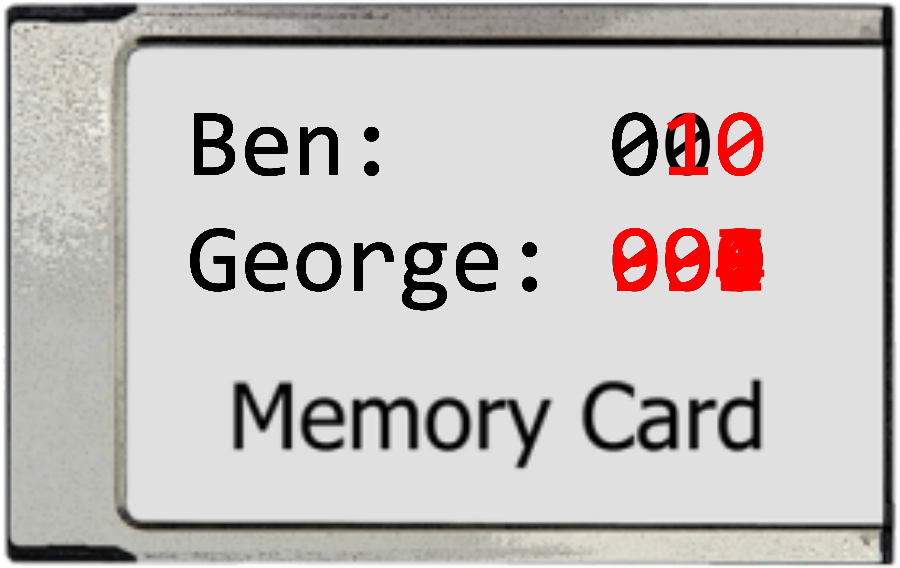
Use only a #2 PENCIL or the marking pen provided.
Do not use red ink! Completely fill in the OVAL.

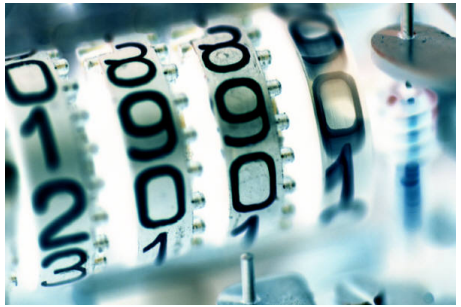

U.S. CONGRESS
(vote for one)
#2 pencil, works everywhere.
S. Rayburn
Black ink, may not work for IR.
J.G. Cannon
Blue ink, may not work for IR.
N. Longworth
Red ink, may not work for IR,
will not work for red!
(write in)


infrared
visible
ultraviolet
1000
800
700
600
500
400
300
wavelength, nanometers


OFFICIAL BALLOT
Random County, Somestate
INSTRUCTIONS: To vote for a candidate, fill in the oval to the left of the name. Use pencil or black ink!
PRESIDENT
(vote for one)
G. Washington
A. Lincoln
(write in)
U.S. CONGRESS
(vote for one)
S. Rayburn
J.G. Cannon
N. Longworth
(write in)

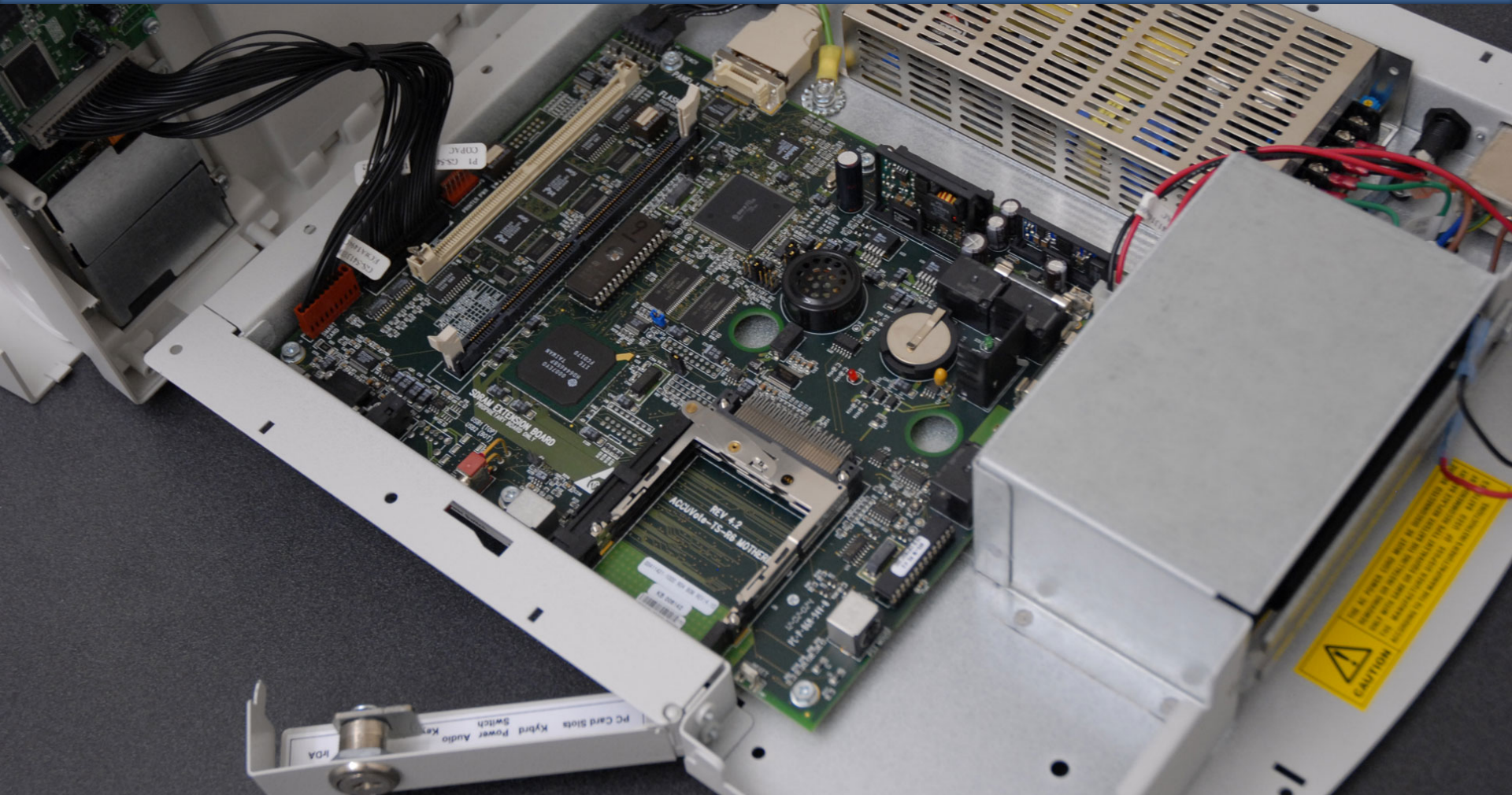

15741
15737
15742
15738
Harri Hursti

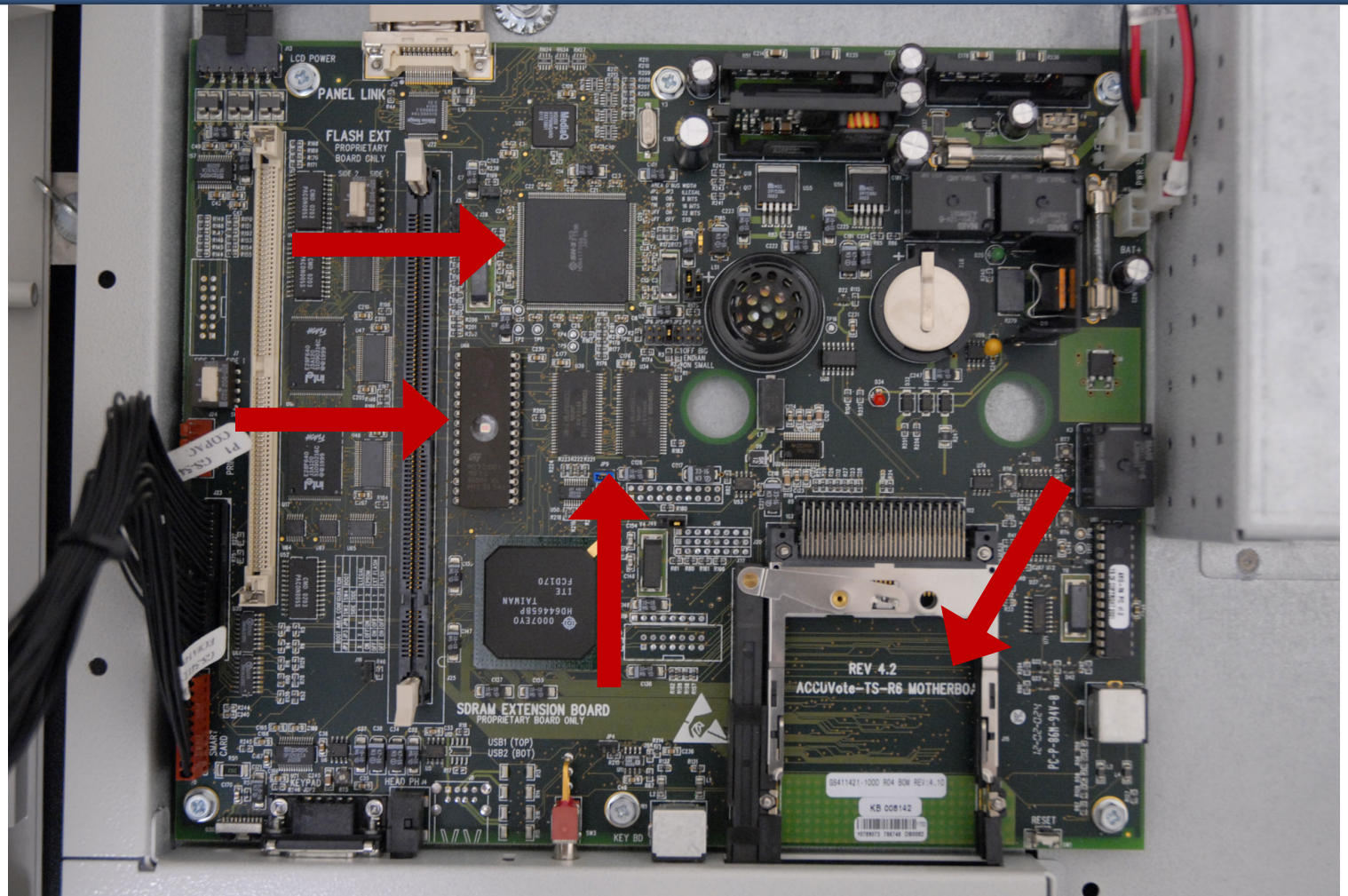

Ben: 010
George: 004
Memory Card

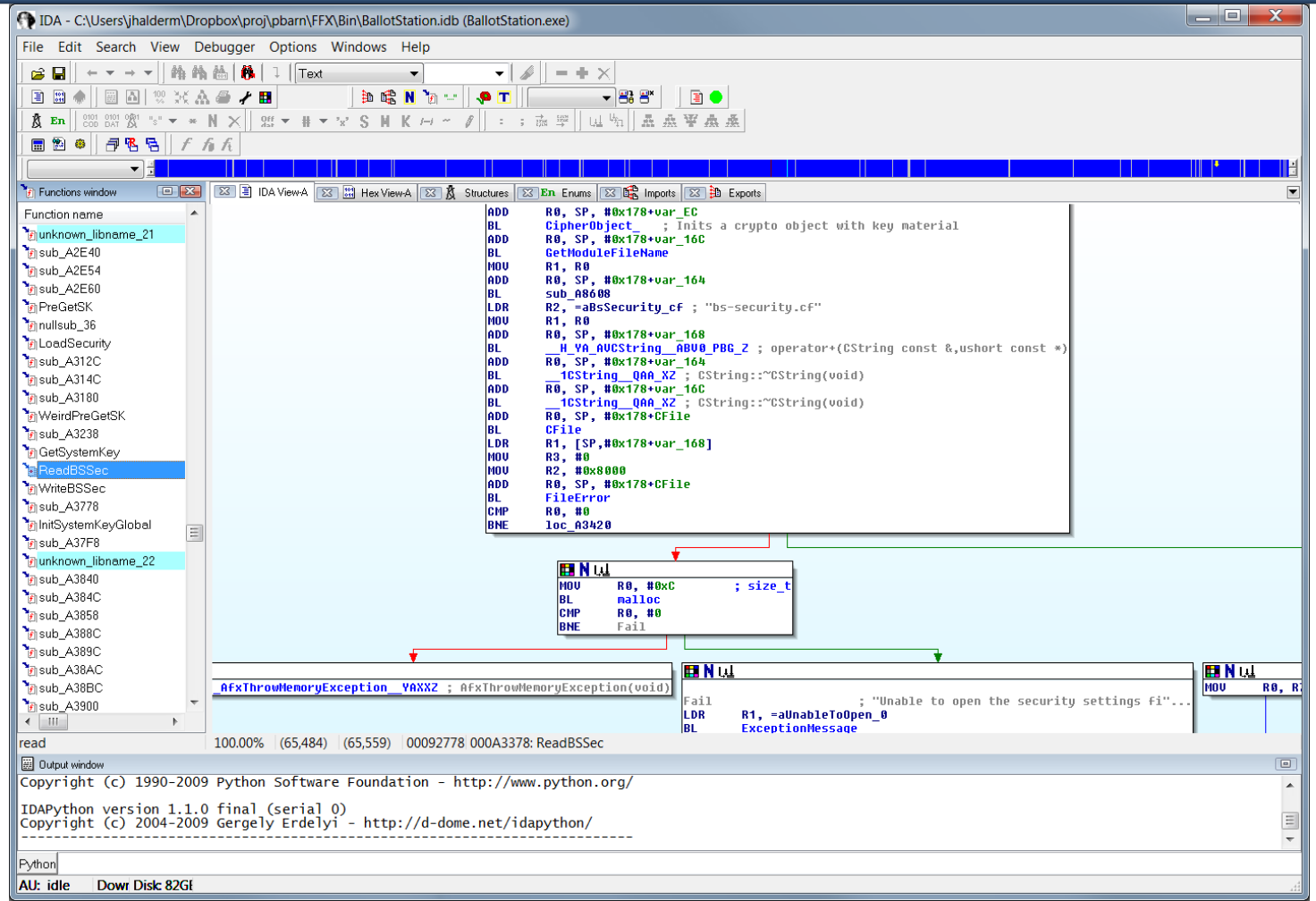


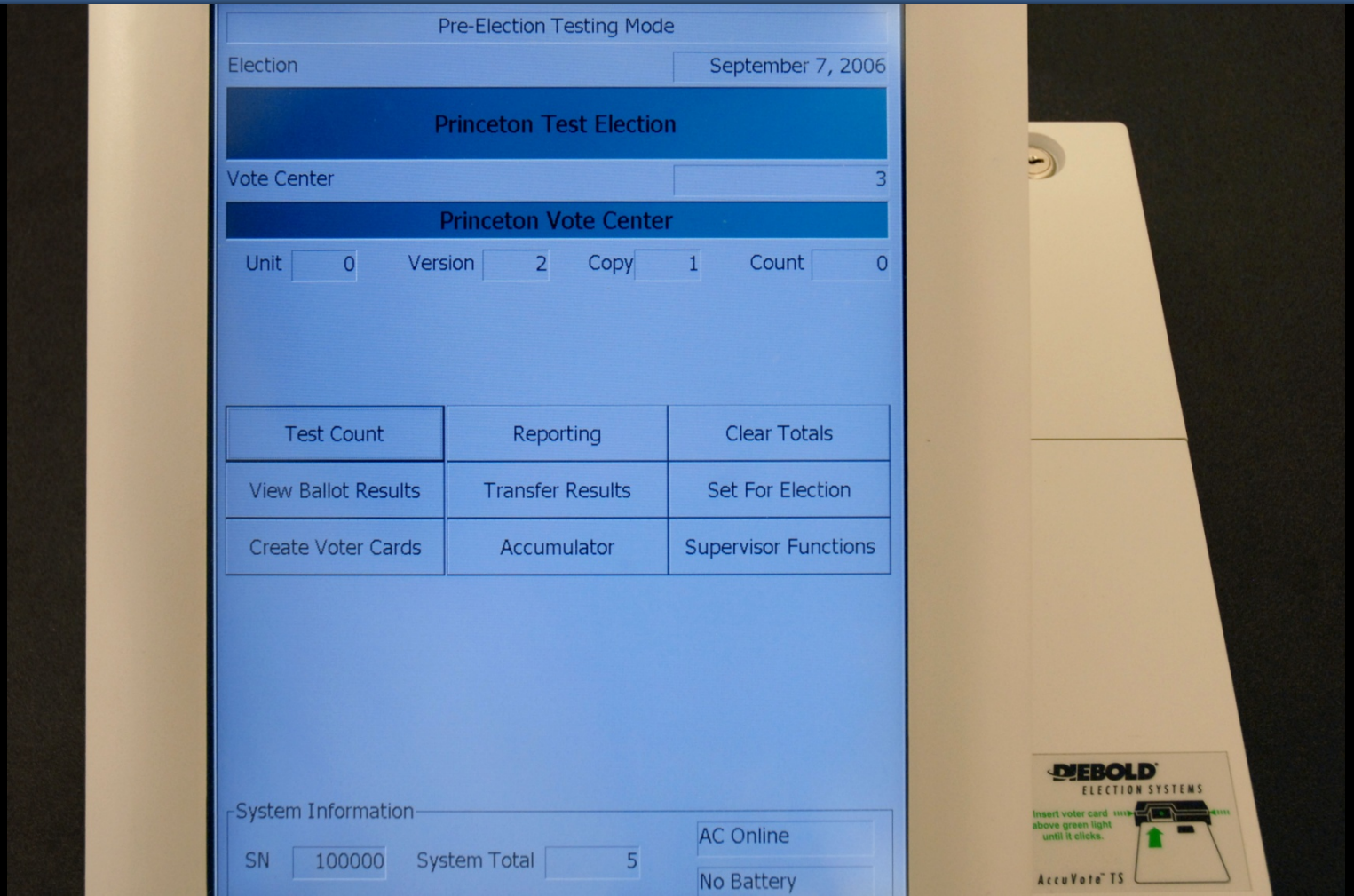
Diebold DREs

Diebold AccuVote-TS

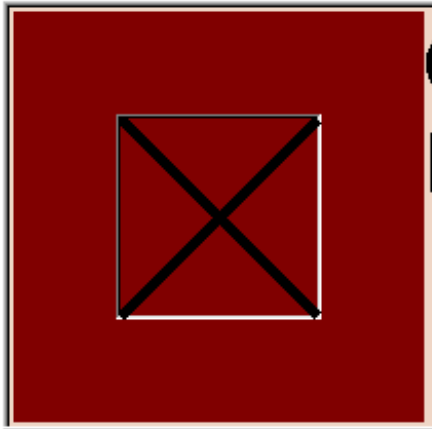

SHRAM EXTENSION BOARD
REV 4.2
ACCUVote-TS-R6 MOTHER
CAUTION


LCD POWER
PANEL LINK
FLASH EXT
PROPRIETARY
BOARD ONLY
SDRAM EXTENSION BOARD
PROPRIETARY BOARD ONLY
USB1 (TOP)
USB2 (BOT)
REV 4.2
ACCUVote-TS-R6 MOTHERBO
KB 008142
RESET


IDA - C:\Users\jhalderm\Dropbox\proj\pbarn\FFX\Bin\BallotStation.idb (BallotStation.exe)
File Edit Search View Debugger Options Windows Help
Functions window
Function name
unknown_libname_21
sub_A2E40
sub_A2E54
sub_A2E60
PreGetSK
nullsub_36
LoadSecurity
sub_A312C
sub_A314C
sub_A3180
WeirdPreGetSK
sub_A3238
GetSystemKey
ReadBSSec
WriteBSSec
sub_A3778
InitSystemKeyGlobal
sub_A37F8
unknown_libname_22
sub_A3840
sub_A384C
sub_A3858
sub_A388C
sub_A389C
sub_A38AC
sub_A38BC
sub_A3900
IDA View-A
Hex View-A
Structures
Enums
Imports
Exports
ADD R0, SP, #0x178+var_EC
BL CipherObject_ ; Inits a crypto object with key material
ADD R0, SP, #0x178+var_16C
BL GetModuleFileName
MOV R1, R0
ADD R0, SP, #0x178+var_164
BL sub_A8608
LDR R2, =aBsSecurity_cf ; "bs-security.cf"
MOV R1, R0
ADD R0, SP, #0x178+var_168
BL __H_YA_AVCString__ABV0_PBG_Z ; operator+(CString const &,ushort const *)
ADD R0, SP, #0x178+var_164
BL __1CString__QAA_XZ ; CString::~CString(void)
ADD R0, SP, #0x178+var_16C
BL __1CString__QAA_XZ ; CString::~CString(void)
ADD R0, SP, #0x178+CFile
BL CFile
LDR R1, [SP,#0x178+var_168]
MOV R3, #0
MOV R2, #0x8000
ADD R0, SP, #0x178+CFile
BL FileError
CMP R0, #0
BNE loc_A3420
MOV R0, #0xC ; size_t
BL malloc
CMP R0, #0
BNE Fail
AfxThrowMemoryException__YAXXZ ; AfxThrowMemoryException(void)
Fail ; "Unable to open the security settings fi"...
LDR R1, =aUnableToOpen_0
BL ExceptionMessage
MOV R0, R
read
100.00% (65,484) (65,559) 00092778 000A3378: ReadBSSec
Output window
Copyright (c) 1990-2009 Python Software Foundation - http://www.python.org/
IDAPython version 1.1.0 final (serial 0)
Copyright (c) 2004-2009 Gergely Erdelyi - http://d-dome.net/idapython/
Python
AU: idle Down Disk 82GB

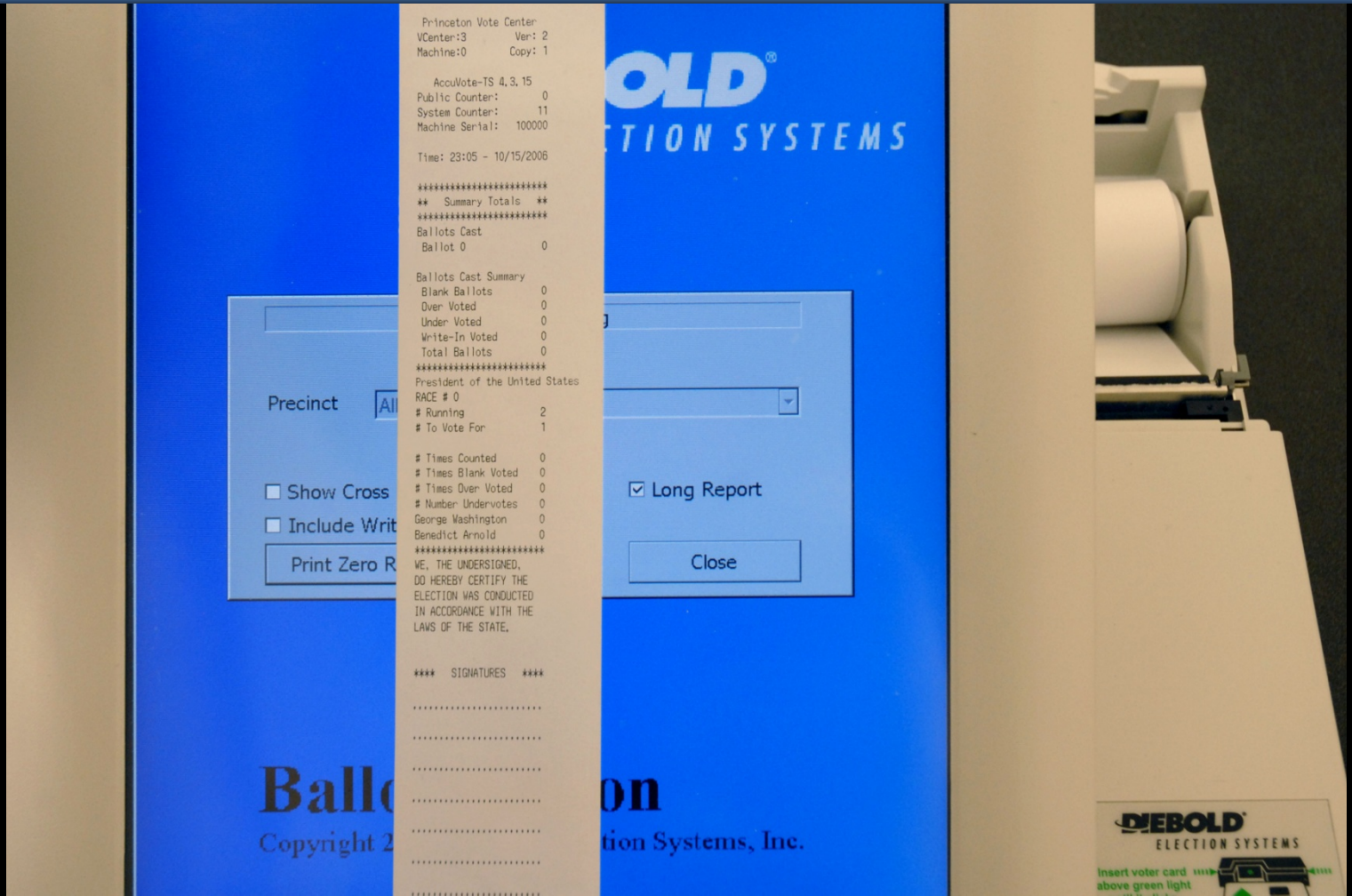

Pre-Election Testing Mode
Election
September 7, 2006
Princeton Test Election
Vote Center
3
Princeton Vote Center
Unit
0
Version
2
Copy
1
Count
0
Test Count
Reporting
Clear Totals
View Ballot Results
Transfer Results
Set For Election
Create Voter Cards
Accumulator
Supervisor Functions
System Information
SN
100000
System Total
5
AC Online
No Battery
DIEBOLD
ELECTION SYSTEMS
Insert voter card above green light until it clicks.
AccuVote TS

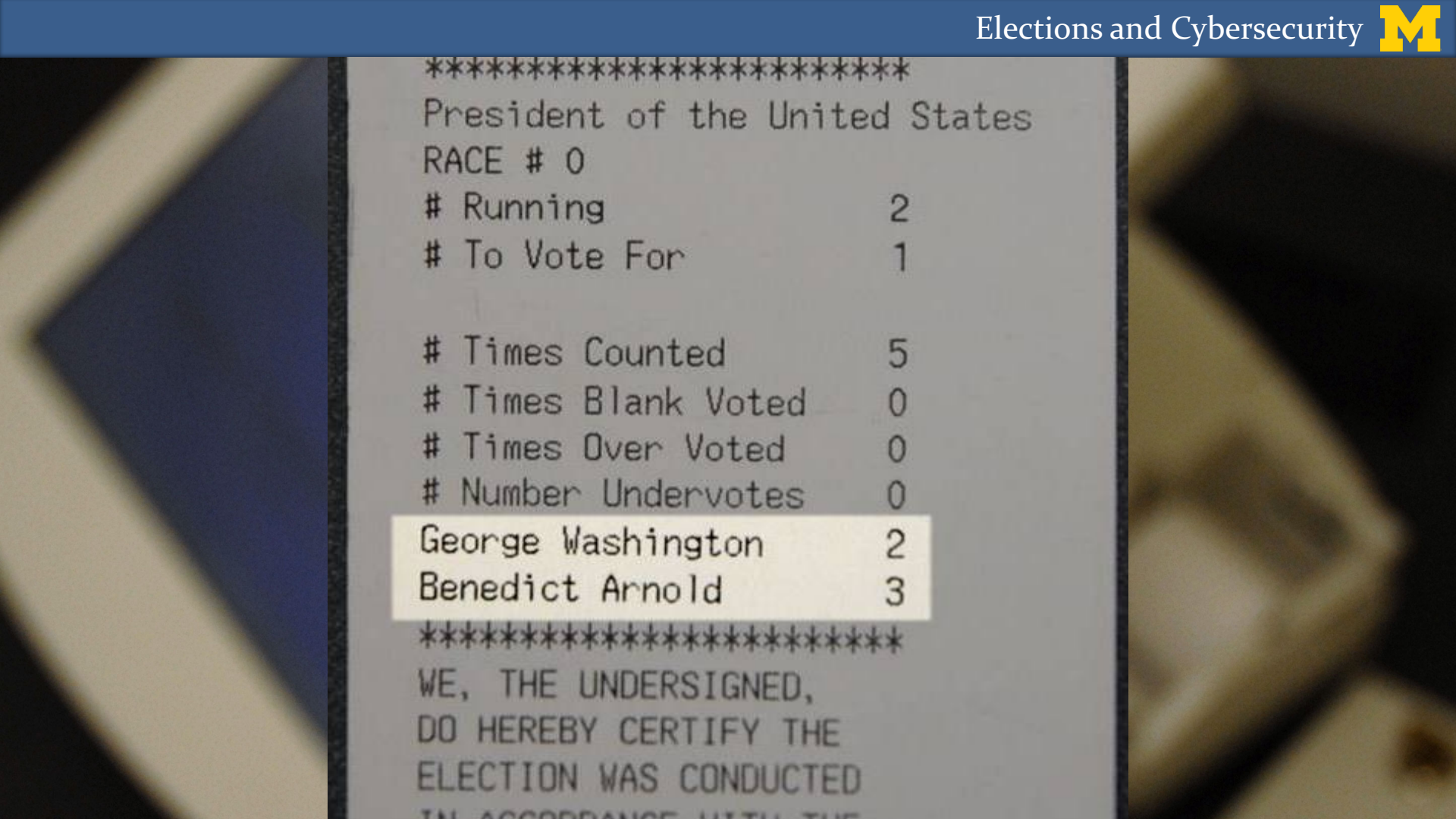
President of the United States

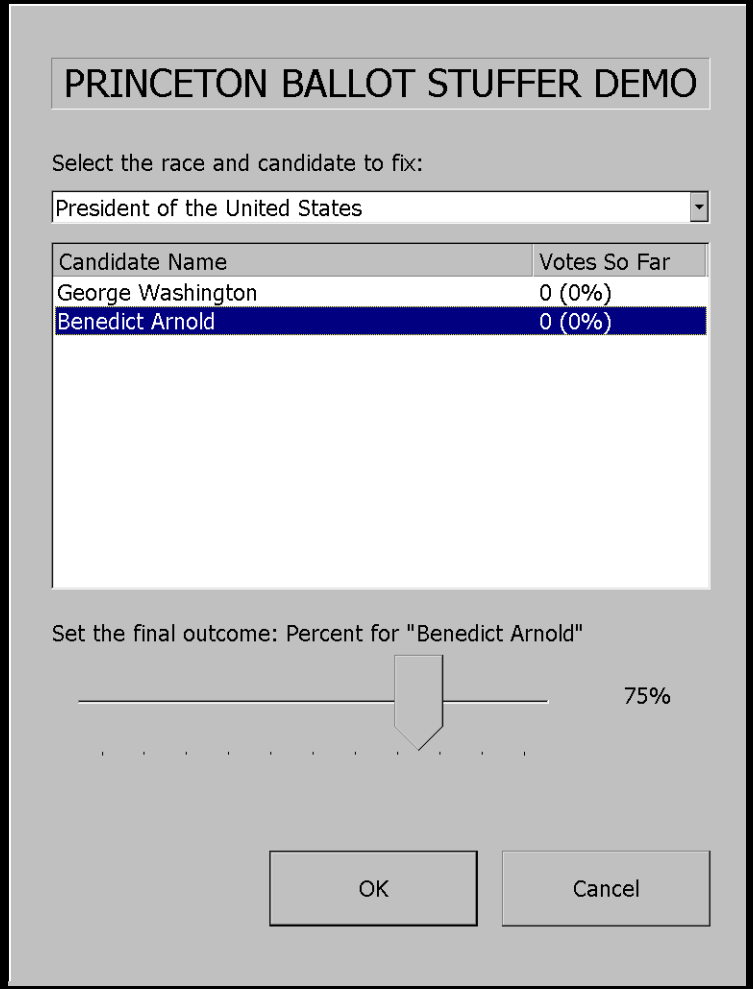


George Washington
Framers Party

Benedict Arnold
Redcoat Party


Princeton Vote Center
VCenter:3 Ver: 2
Machine:0 Copy: 1
AccuVote-TS 4.3.15
Public Counter: 0
System Counter: 11
Machine Serial: 100000
Time: 23:05 - 10/15/2006
** Summary Totals **
Ballots Cast
Ballot 0 0
Ballots Cast Summary
Blank Ballots 0
Over Voted 0
Under Voted 0
Write-In Voted 0
Total Ballots 0
President of the United States
RACE # 0
Running 2
To Vote For 1
Times Counted 0
Times Blank Voted 0
Times Over Voted 0
Number Undervotes 0
George Washington 0
Benedict Arnold 0
WE, THE UNDERSIGNED,
DO HEREBY CERTIFY THE
ELECTION WAS CONDUCTED
IN ACCORDANCE WITH THE
LAWS OF THE STATE.
**** SIGNATURES ****
Precinct
Show Cross
Include Writ
Print Zero R
Long Report
Close
TION SYSTEMS
Copyright 2
tion Systems, Inc.
DIEBOLD
ELECTION SYSTEMS
Insert voter card
above green light

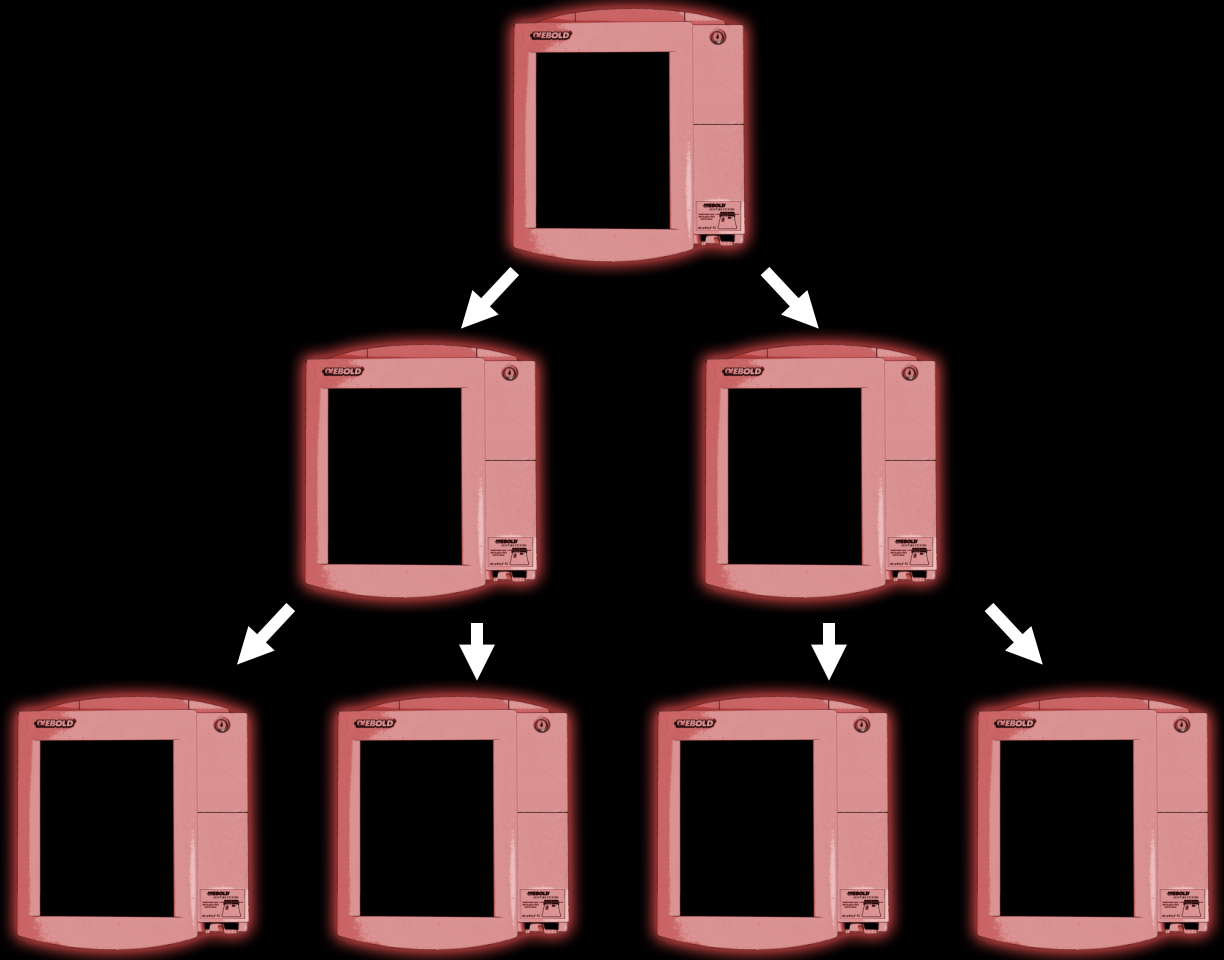

****
President of the United States
RACE # 0
Running 2
To Vote For 1
Times Counted 5
Times Blank Voted 0
Times Over Voted 0
Number Undervotes 0
George Washington 2
Benedict Arnold 3
****
WE, THE UNDERSIGNED,
DO HEREBY CERTIFY THE
ELECTION WAS CONDUCTED


PRINCETON BALLOT STUFFER DEMO
Select the race and candidate to fix:
President of the United States
Candidate Name
Votes So Far
George Washington
0 (0%)
Benedict Arnold
0 (0%)
Set the final outcome: Percent for "Benedict Arnold"
75%
OK
Cancel


DIEBOLD
ry Card


Memory Card


DIEBOLD


DIEBOLD


DIEBOLD
Keypad
Audio


DIEBOLD
IrDA
Keypad
Audio


Automatic Refreshment Centre
by BARTECH
WICHTIG
IMPORTANT
IMPORTANTE
Coors
LIGHT
Coca-Cola
Coke

- Transfer & Transport Cases
- DIMS-NeT/Voter Registration
- Voting Booths & Ballot Boxes

Replacement Access Keys

- 2 keys that allow easy service access to the Tally Printer and replacement battery compartment

GS-567311-1000 **$5.90** USD per set
$6.90 CAD per set

Enter a quantity

add to your order ▸

ORDER BY PHONE 800.769.3246

More Goes Wrong

Hart

Sequoia

Diebold

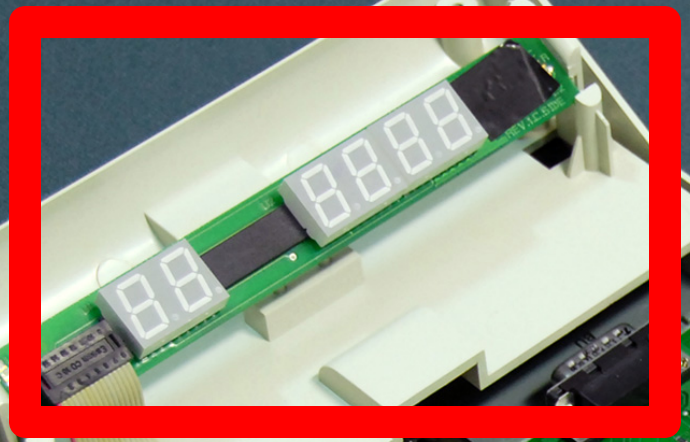

JUSTIÇA
ELEITORAL
Lei nº 10.826, de 22/12/2003
O comércio de armas de fogo e munição deve ser proibido no Brasil?
1 - SIM
2 - NÃO
1 2 3
4 5 6
7 8 9
0
BRANCO
CORRIGE
CONFIRMA
PROCOMP

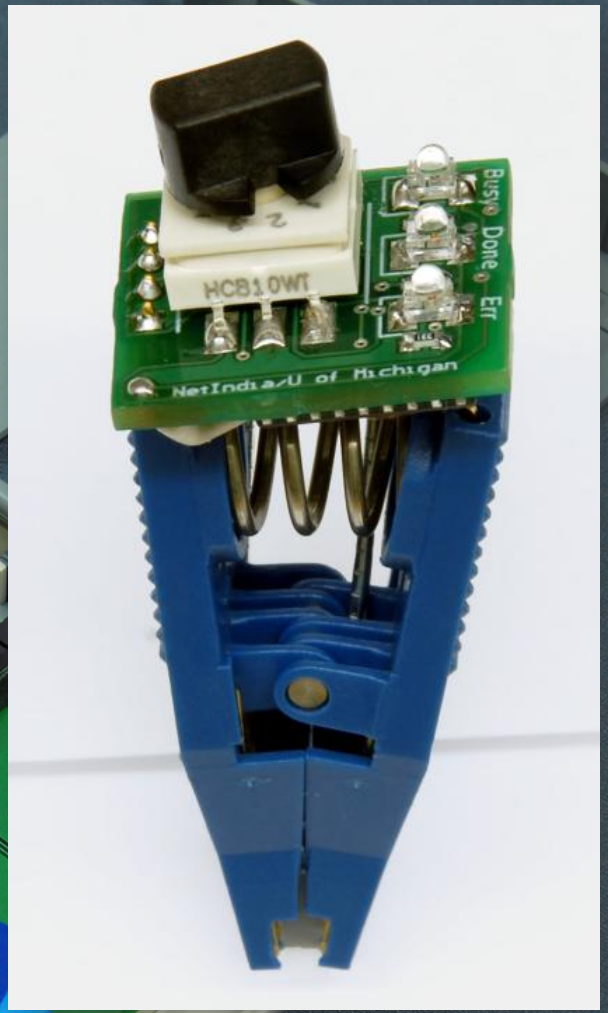
Brazil, too?


1. AVATAR
2. BOBBY
3. CHAND
4. DAVID
5. ESWAR
6.
ON
Sl.No.
Votes
Busy
Total
Ballot
Control Unit

Et tu, India?


1. AVATAR
2. BOBBY
3. CHAND
4. DAVID
ON
SL.No.
Votes
BUSY




HCB1.0WT
Busy
Done
Err
NetIndia/U of Michigan

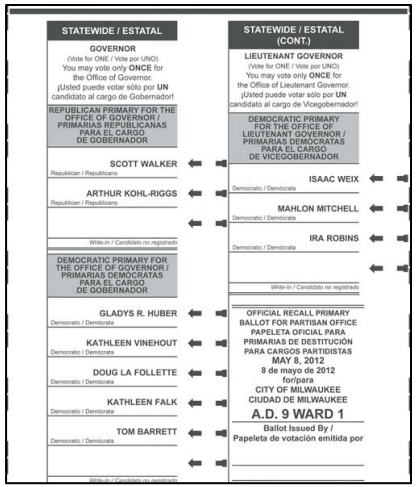
Bonus: Sequoia AVC Edge


TOUCH
YOU MAY CHANGE
WRITE-IN
CONTINUE
REVIEW
COMPLETE
PAC-MAN
PAC-MAN on the Sequoia AVC Edge DRE voting machine

Post-Election Auditing


N
W
E
S

Keep Redundant Records



AUDIT =?

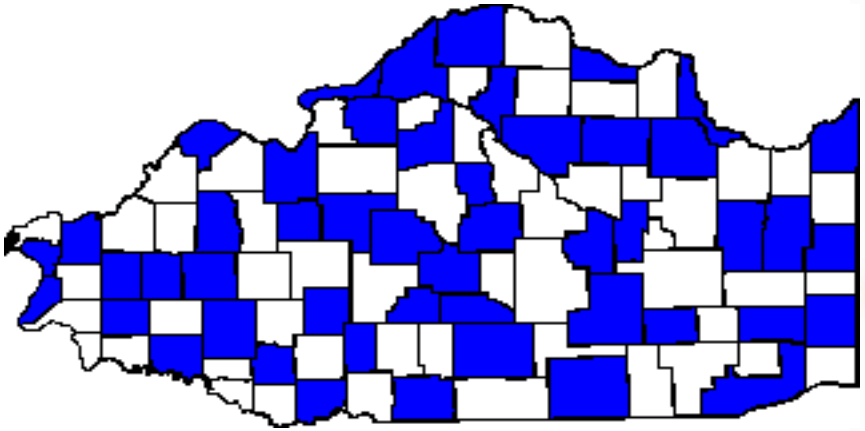
Slow/ex tally

Verified by voter Unverified

Redundancy + Different failure modes = Greater security

But…Redundancy only helps if we use both records!

Post-Election Audits



Pick some precincts **randomly** for paper recount.

If electronic tallies disagree, recount everywhere.

How much to Audit?

Standard practice:

Fixed Fraction of Precincts
(e.g., 10%)

Recommended practice:

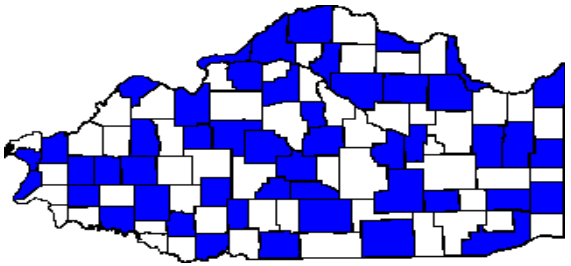
Fixed Level of Confidence
(e.g., 99%)

Statistical Risk-Limiting Audits

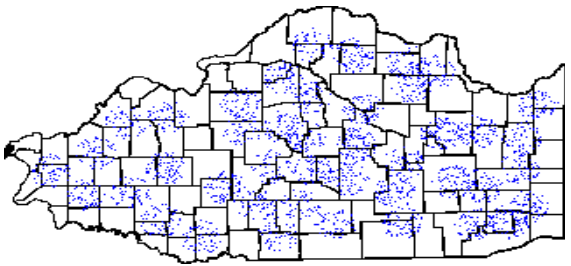
Goal: Establish, with high statistical confidence, that hand-counting *all* of the paper records would yield the same winner as the electronic tally.

An Alternative Approach

Precinct-based auditing
(standard practice)



Ballot-based auditing



100 marbles, 10% blue (fraud)

6300 beads, 10% blue (fraud)

How large a sample do we need to detect an error?
It depends…

Why is Ballot-based auditing hard?

325631 Alice
218594 Bob
810581 Alice

● Alice
○ Bob
325631

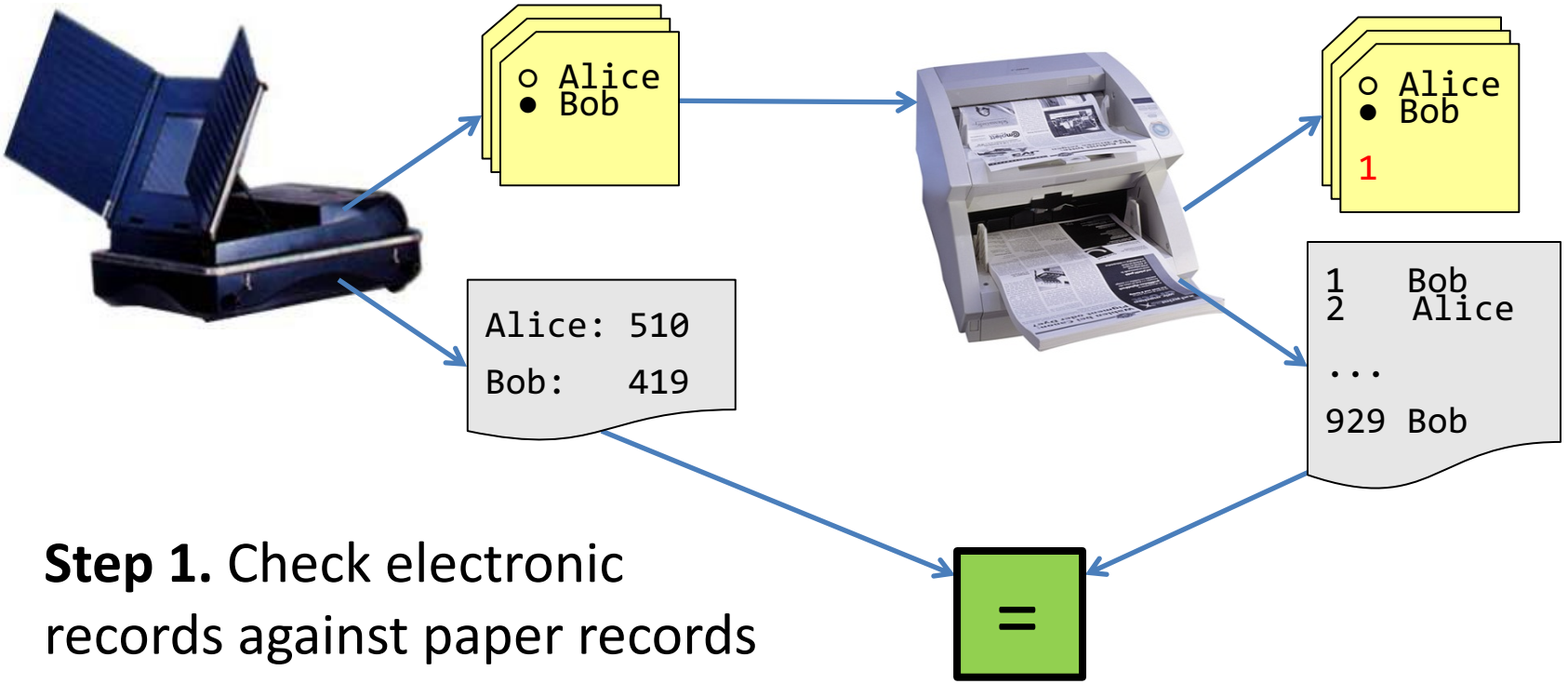
○ Alice
● Bob
218594

● Alice
○ Bob
810581

Need to match up electronic with paper ballots.

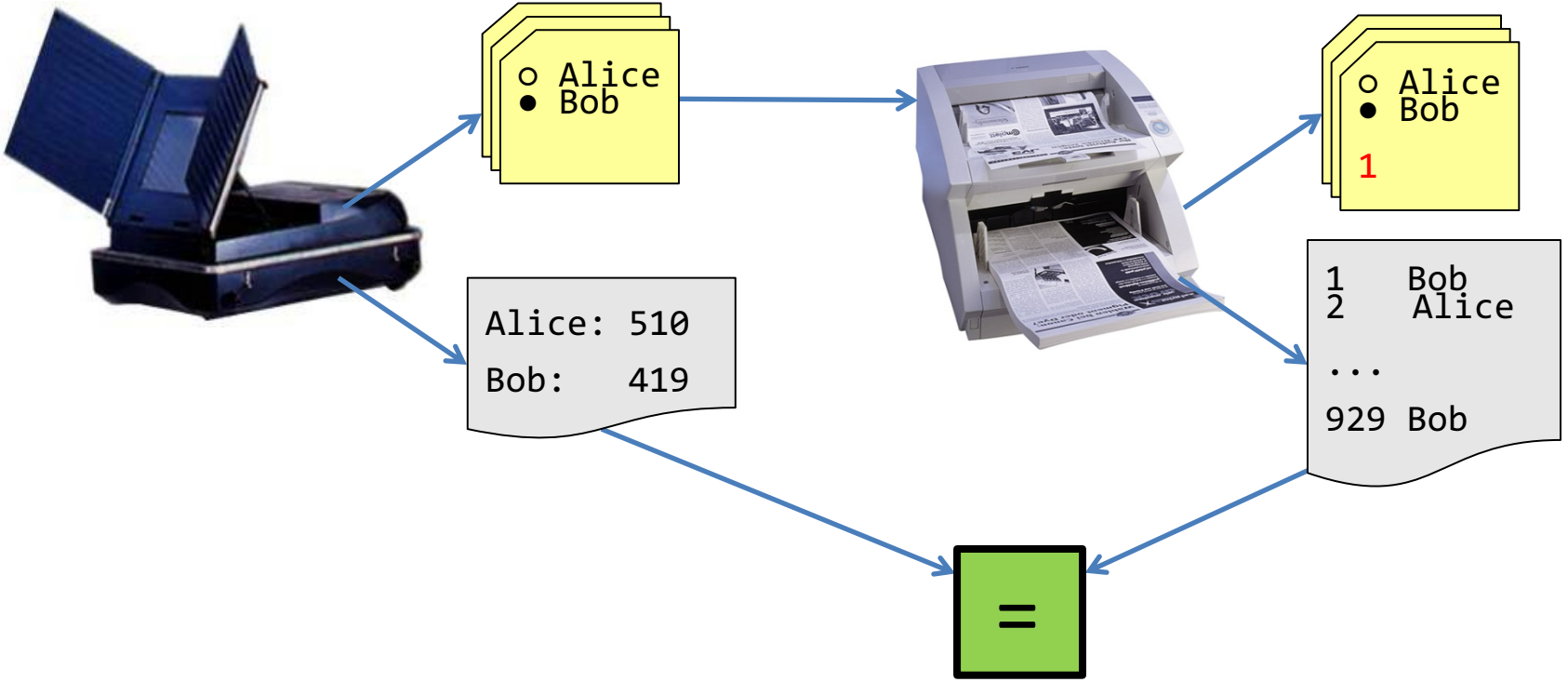
Difficult without compromising the secret ballot!

Machine-Assisted Auditing

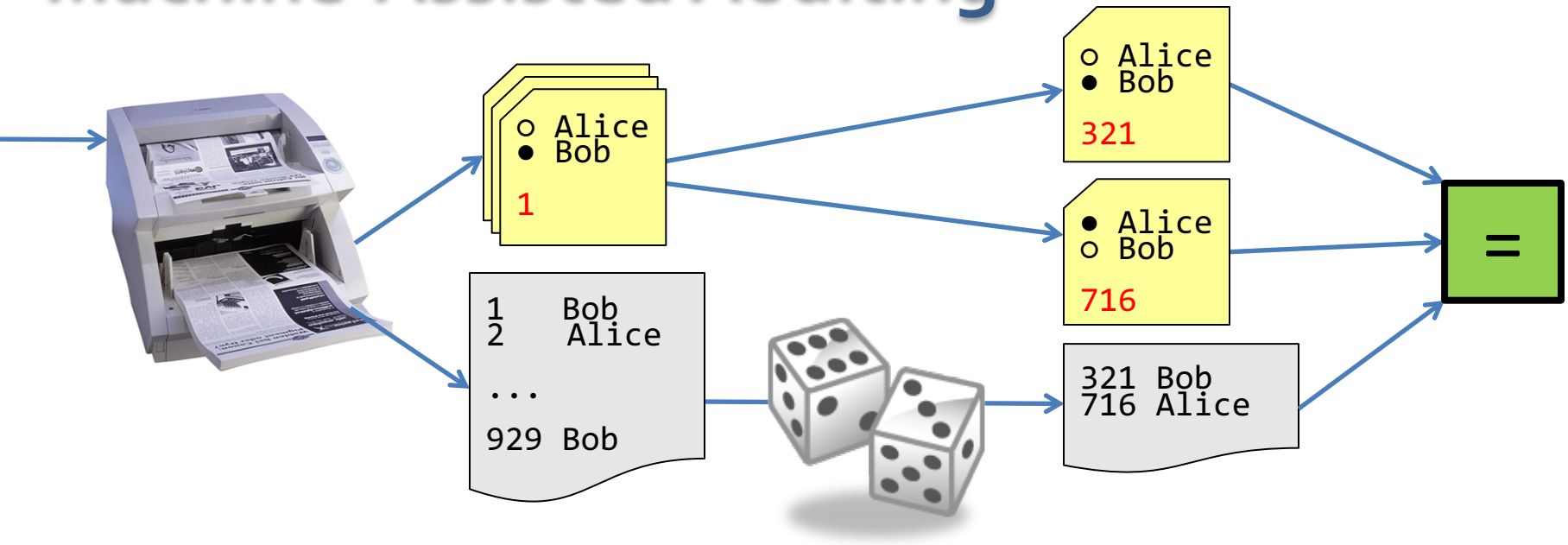


Step 1. Check electronic records against paper records using a **recount machine**.

Machine-Assisted Auditing

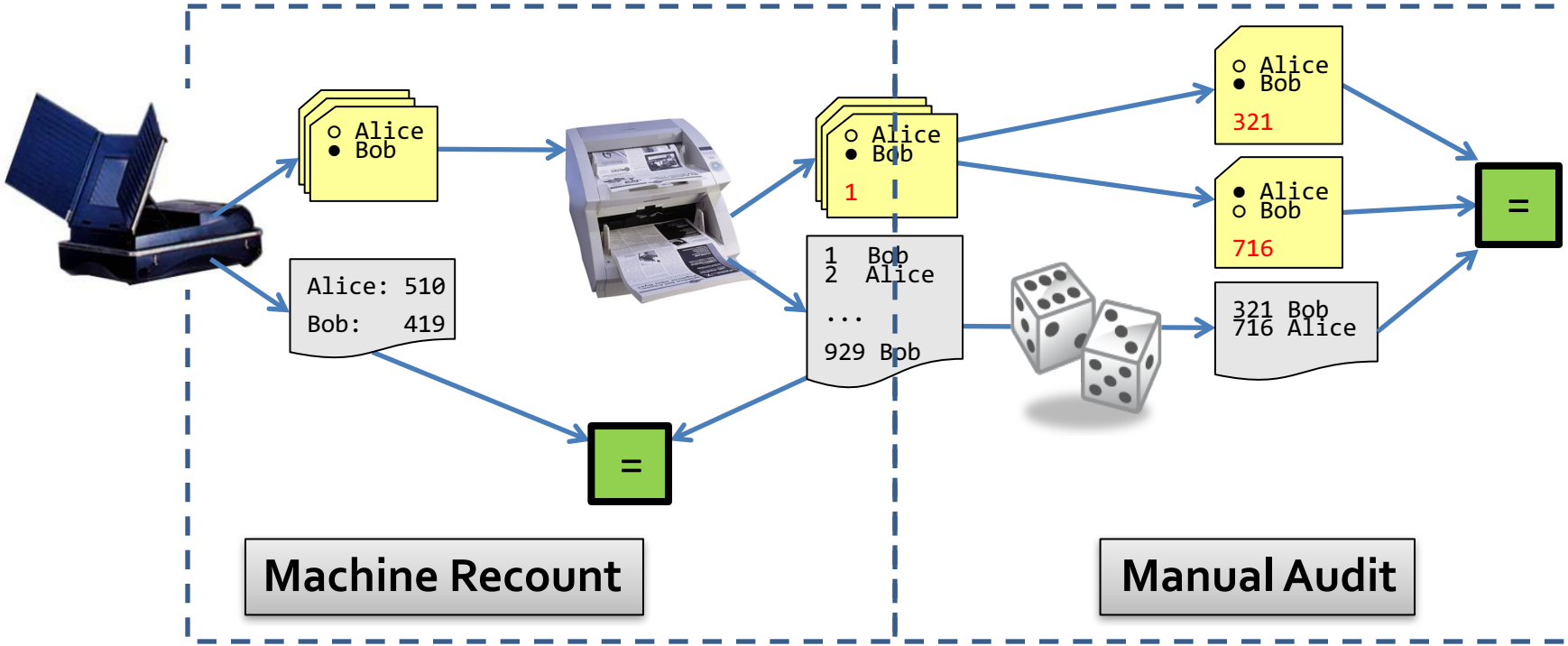


Machine-Assisted Auditing



Step 2. Audit the recount machine by selecting random ballots for human inspection.

Machine-Assisted Auditing



We can use a machine without having to trust it!

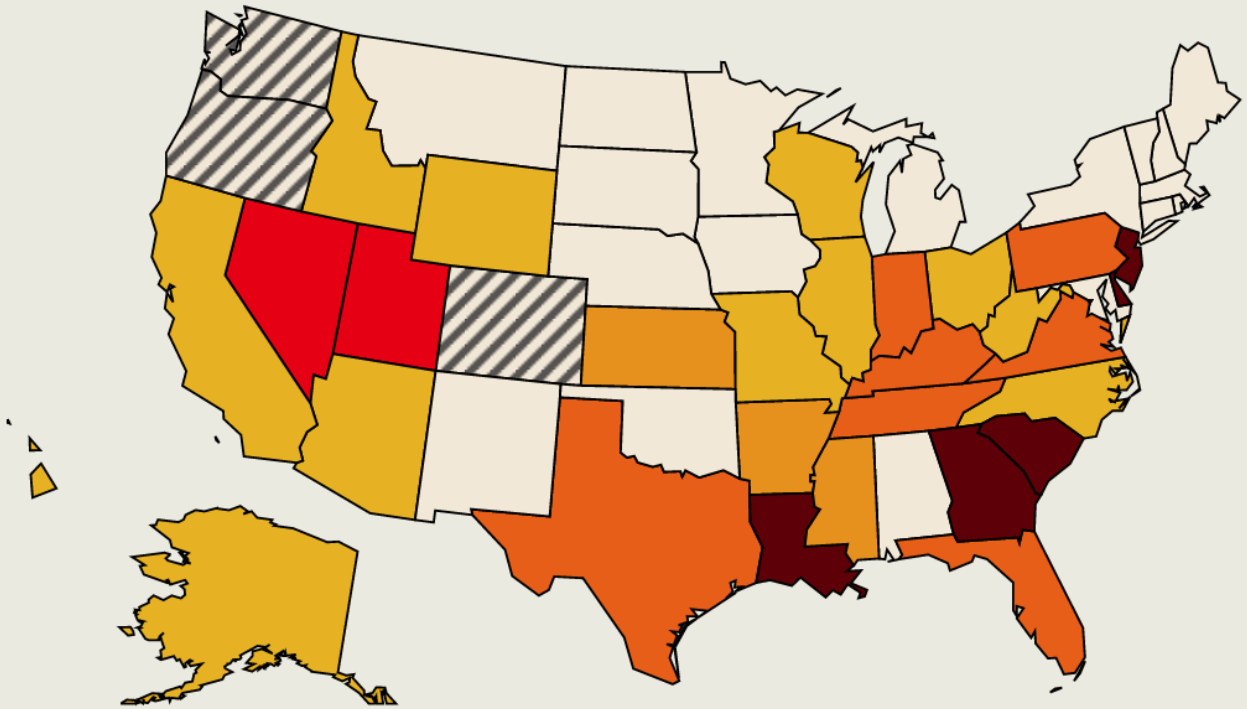
The Gold-Medal Standard

Precinct-Count Optical Scan

+

Mandatory Risk-Limiting Audits

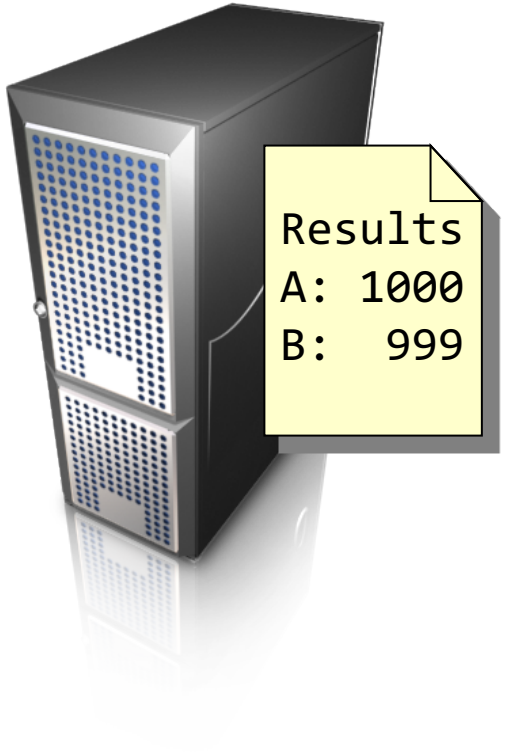
In 2016, **30% of American voters** have no physical record of their vote.



- Paper Ballot
- All Vote By Mail
- Paper Ballot and Punch Card
- Mixed Paper Ballot and DREs with VVPAT
- Mixed Paper Ballot and DREs with and without VVPAT
- Mixed Paper Ballot and DREs without VVPAT
- DREs with VVPAT
- DREs with and without VVPAT
- DREs without VVPAT

Internet Voting?

Server-side Threats



- Denial of Service
- Remote Intrusion
- Insider Attacks
- State-Sponsored Attacks

Client-side Threats

- Credential Theft
- Imposter Sites
- Malware

Case Study

Washington, D.C. (2010)

DISTRICT OF COLUMBIA
BOARD OF ELECTIONS AND ETHICS
WASHINGTON, D.C. 20001-2745

MEDIA RELEASE

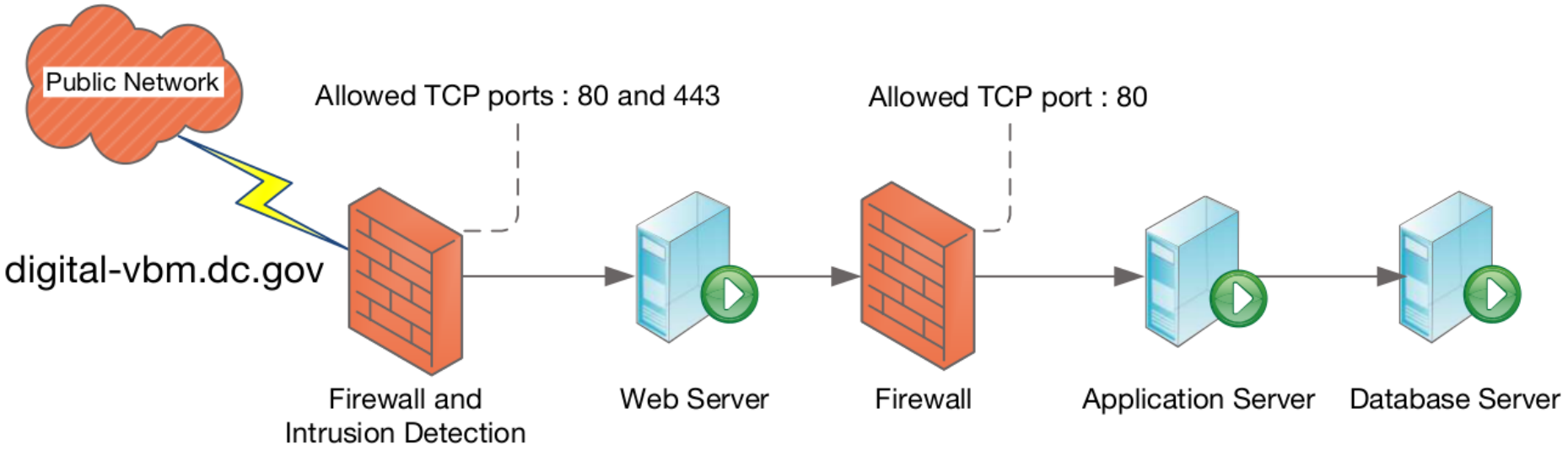
D.C. BOARD OF ELECTIONS AND ETHICS
September 21, 2010

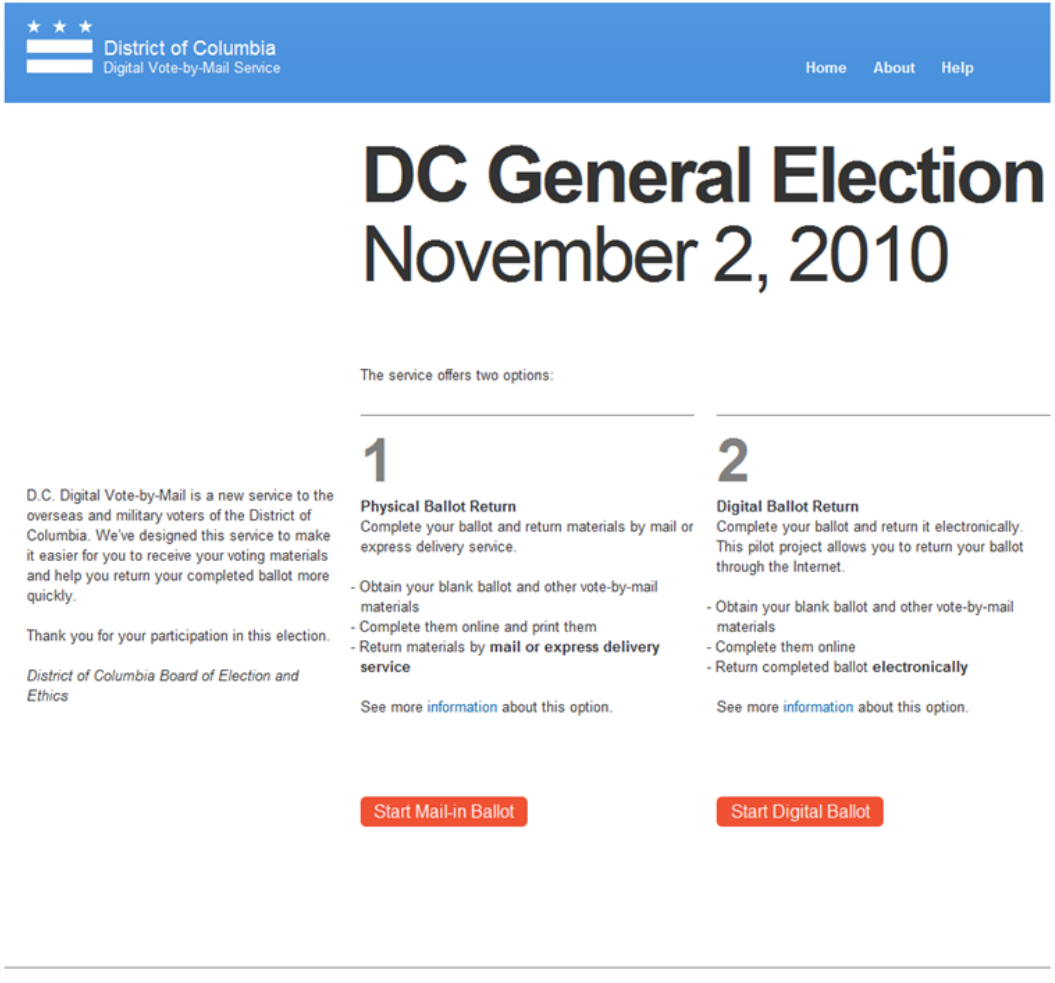
Contact: Alysoun McLaughlin, amclaughlin@dcboee.org
202-727-2511 (direct)/202-441-1121 (cell)

Board Announces Public Test of Digital Vote by Mail Service

Open Source Solution Provides Secure Alternative for Overseas Voters Who Are Underserved by Traditional Vote by Mail

WASHINGTON, D.C. —The Board of Elections and Ethics today announced that the public examination phase of the Digital Vote by Mail pilot project for overseas voters will begin on Friday, September 24.


Public Network
Allowed TCP ports : 80 and 443
Allowed TCP port : 80
digital-vbm.dc.gov
Firewall and
Intrusion Detection
Web Server
Firewall
Application Server
Database Server



District of Columbia
Digital Vote-by-Mail Service

Home About Help

DC General Election
November 2, 2010

D.C. Digital Vote-by-Mail is a new service to the overseas and military voters of the District of Columbia. We've designed this service to make it easier for you to receive your voting materials and help you return your completed ballot more quickly.

Thank you for your participation in this election.

District of Columbia Board of Election and Ethics

The service offers two options:

1

Physical Ballot Return
Complete your ballot and return materials by mail or express delivery service.

- Obtain your blank ballot and other vote-by-mail materials
- Complete them online and print them
- Return materials by **mail or express delivery service**

See more information about this option.

Start Mail-in Ballot

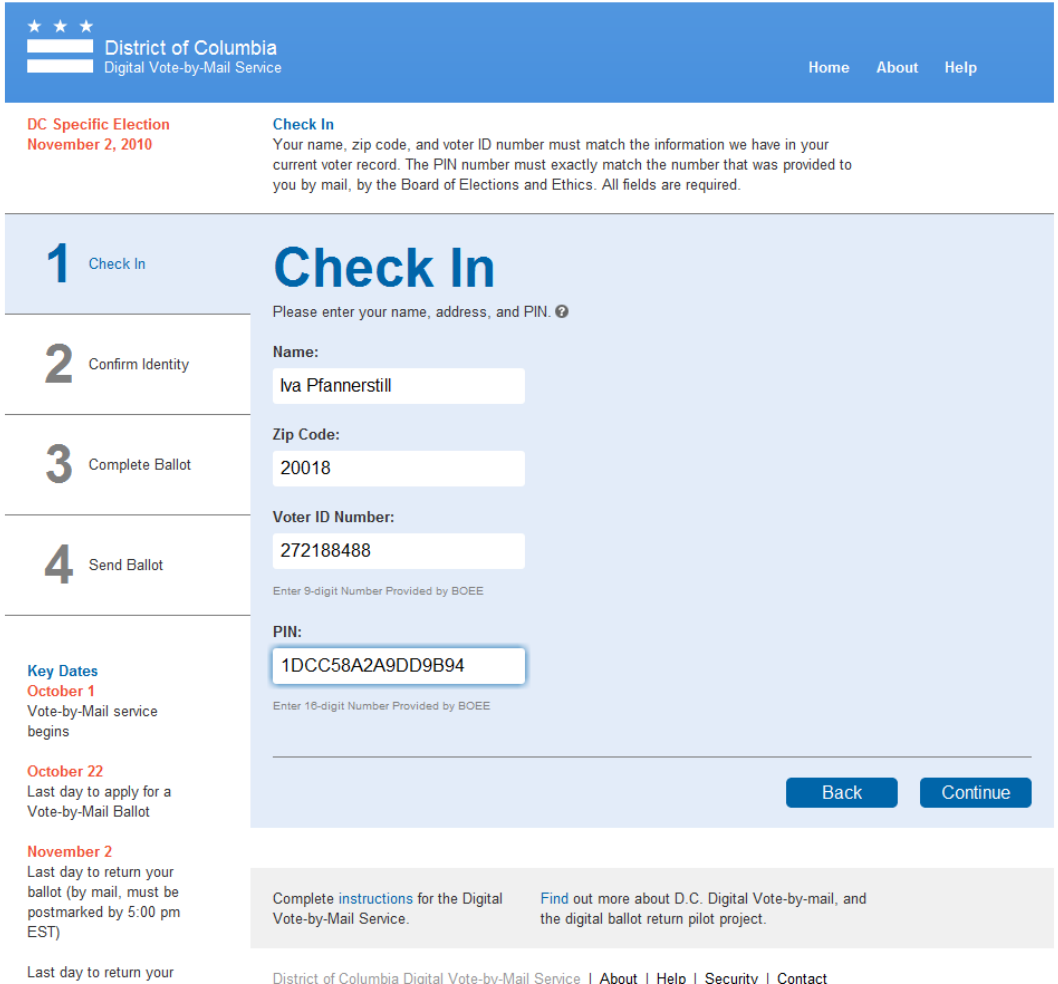
2

Digital Ballot Return
Complete your ballot and return it electronically. This pilot project allows you to return your ballot through the Internet.

- Obtain your blank ballot and other vote-by-mail materials
- Complete them online
- Return completed ballot **electronically**

See more information about this option.

Start Digital Ballot


District of Columbia
Digital Vote-by-Mail Service
Home
About
Help
DC Specific Election
November 2, 2010
Check In
Your name, zip code, and voter ID number must match the information we have in your current voter record. The PIN number must exactly match the number that was provided to you by mail, by the Board of Elections and Ethics. All fields are required.
1 Check In
2 Confirm Identity
3 Complete Ballot
4 Send Ballot
Check In
Please enter your name, address, and PIN.
Name:
Iva Pfannerstill
Zip Code:
20018
Voter ID Number:
272188488
Enter 9-digit Number Provided by BOEE
PIN:
1DCC58A2A9DD9B94
Enter 16-digit Number Provided by BOEE
Back
Continue
Key Dates
October 1
Vote-by-Mail service begins
October 22
Last day to apply for a Vote-by-Mail Ballot
November 2
Last day to return your ballot (by mail, must be postmarked by 5:00 pm EST)
Last day to return your
Complete instructions for the Digital Vote-by-Mail Service.
Find out more about D.C. Digital Vote-by-mail, and the digital ballot return pilot project.
District of Columbia Digital Vote-by-Mail Service | About | Help | Security | Contact

District of Columbia
Digital Vote-by-Mail Service

Home About Help

DC Specific Election
November 2, 2010

Complete Ballot
Digital ballot return lets you return your ballot electronically. You will need to save your marked ballot, locate it on your computer, and upload it to the BOEE. Keep this page open until you have saved your completed ballot.

1 Check In
2 Confirm Identity
3 Complete Ballot
4 Send Ballot

Download

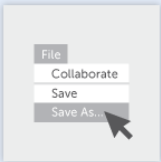
Download and View Your Ballot
Click the PDF icon at the right to download your ballot. The ballot PDF will open in your default PDF viewing application, on top of your web browser.

Mark

Mark Your Ballot
To complete the ballot online, click on the circles next to your candidates to select them. You can also type in candidates where indicated.

Save

Save Your Ballot
You must save your ballot when you have marked it. Save the PDF on your computer by selecting File/Save As in your default PDF viewing application. Save the ballot to a place where you can easily find it again (for example, your desktop). Do NOT rename the ballot.



Back Continue

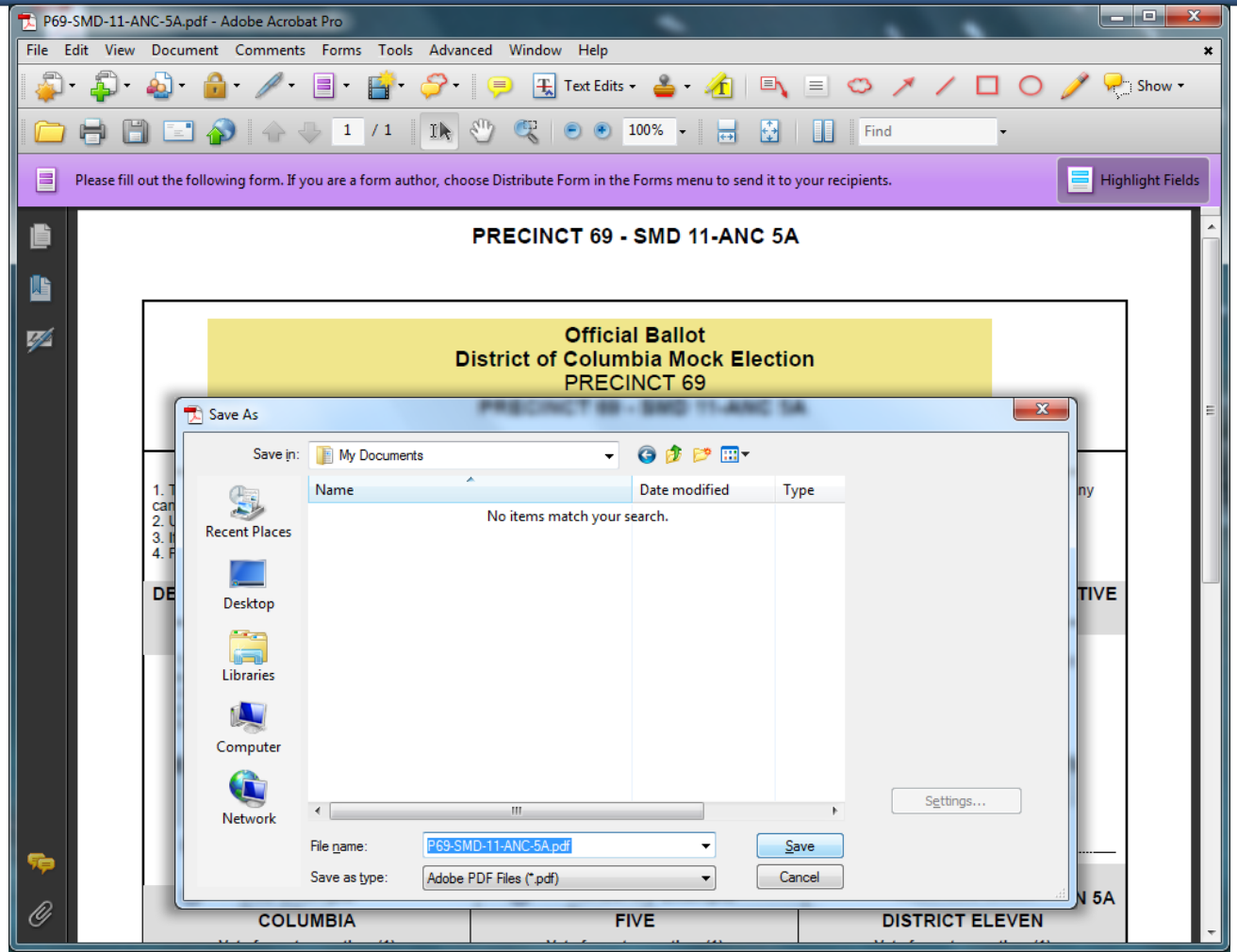
Key Dates

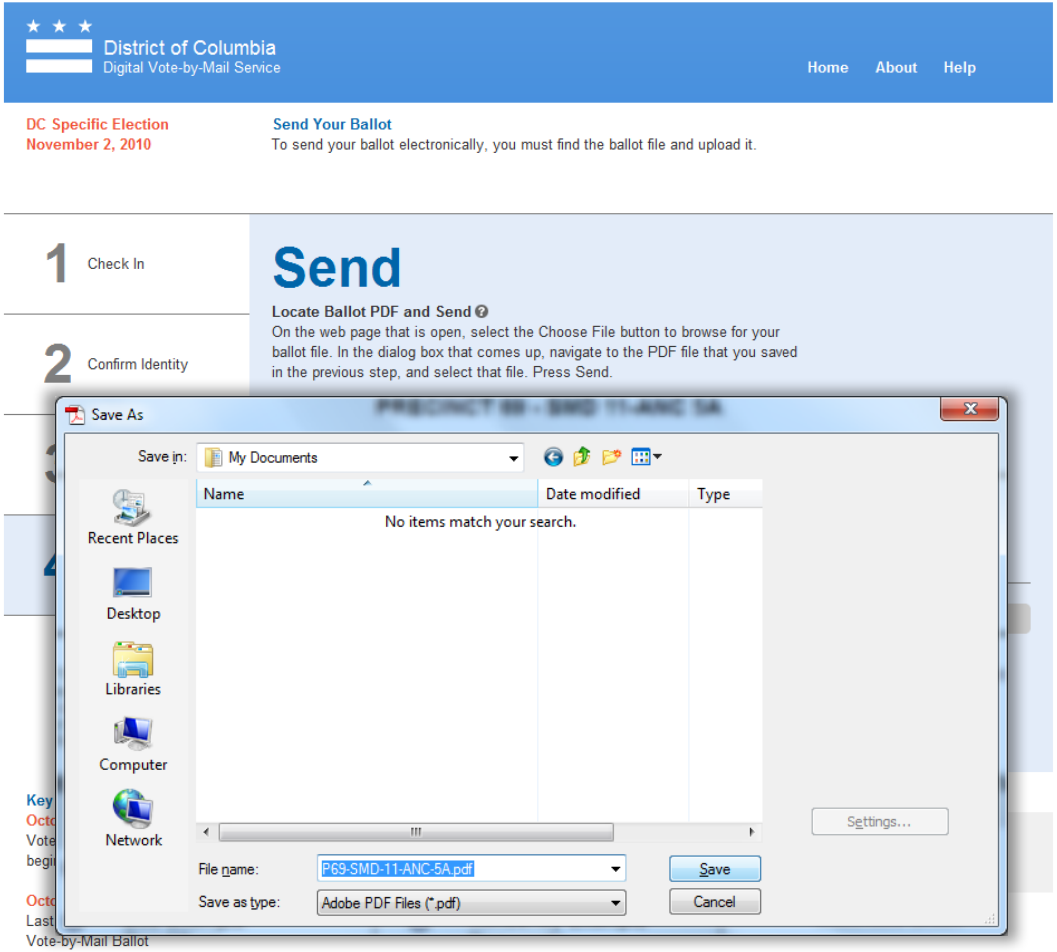
October 1
Vote-by-Mail service begins

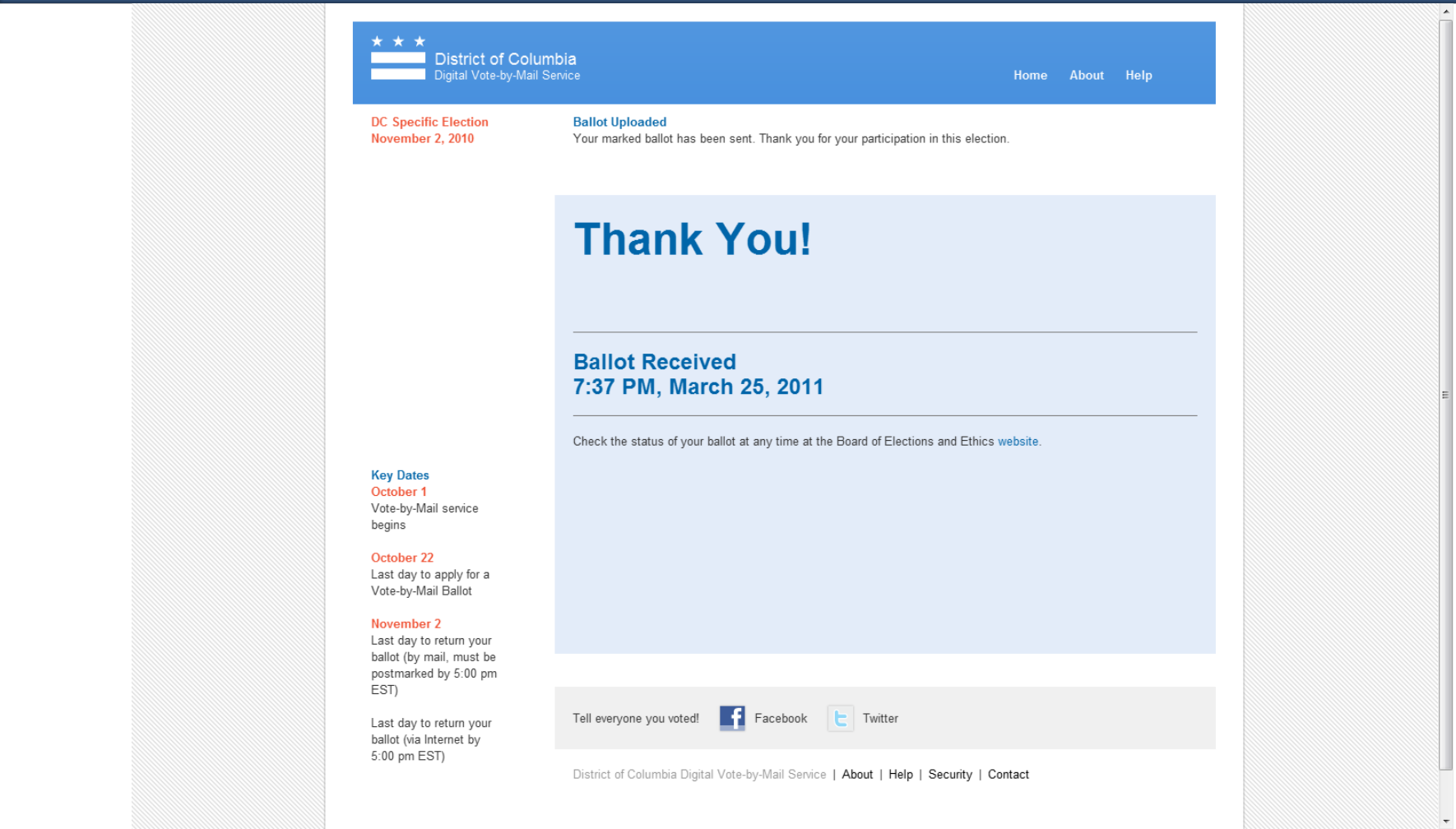
October 22
Last day to apply for a Vote-by-Mail Ballot

November 2
Last day to return your ballot (by mail, must be postmarked by 5:00 pm

https://testthevote.org/assets/ballot_styles/P69-SMD-11-ANC-5A.pdf?1285465645


P69-SMD-11-ANC-5A.pdf - Adobe Acrobat Pro
File Edit View Document Comments Forms Tools Advanced Window Help
Please fill out the following form. If you are a form author, choose Distribute Form in the Forms menu to send it to your recipients.
Highlight Fields
PRECINCT 69 - SMD 11-ANC 5A
Official Ballot
District of Columbia Mock Election
PRECINCT 69
Save As
Save in: My Documents
Name
Date modified
Type
No items match your search.
Recent Places
Desktop
Libraries
Computer
Network
Settings...
File name: P69-SMD-11-ANC-5A.pdf
Save as type: Adobe PDF Files (*.pdf)
Save
Cancel
COLUMBIA
FIVE
DISTRICT ELEVEN


District of Columbia
Digital Vote-by-Mail Service
Home
About
Help
DC Specific Election
November 2, 2010
Send Your Ballot
To send your ballot electronically, you must find the ballot file and upload it.
1 Check In
2 Confirm Identity
Send
Locate Ballot PDF and Send
On the web page that is open, select the Choose File button to browse for your ballot file. In the dialog box that comes up, navigate to the PDF file that you saved in the previous step, and select that file. Press Send.
Save As
Save in:
My Documents
Recent Places
Desktop
Libraries
Computer
Network
Name
Date modified
Type
No items match your search.
Settings...
File name:
P69-SMD-11-ANC-5A.pdf
Save as type:
Adobe PDF Files (*.pdf)
Save
Cancel
Vote-by-Mail Ballot



District of Columbia
Digital Vote-by-Mail Service

Home About Help

DC Specific Election
November 2, 2010

Ballot Uploaded
Your marked ballot has been sent. Thank you for your participation in this election.

Thank You!

Ballot Received
7:37 PM, March 25, 2011

Check the status of your ballot at any time at the Board of Elections and Ethics website.

Key Dates

October 1
Vote-by-Mail service begins

October 22
Last day to apply for a Vote-by-Mail Ballot

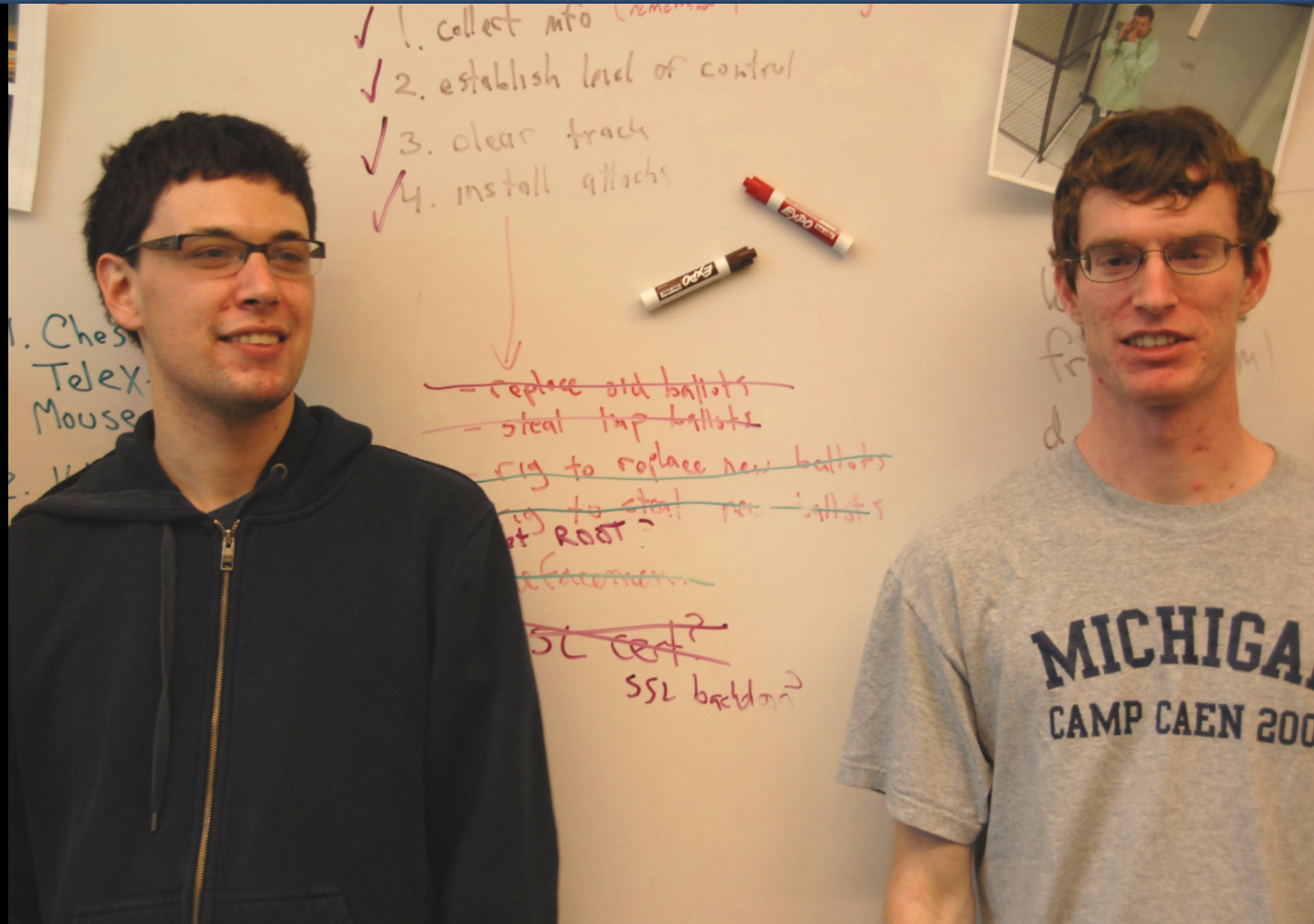
November 2
Last day to return your ballot (by mail, must be postmarked by 5:00 pm EST)

Last day to return your ballot (via Internet by 5:00 pm EST)

Tell everyone you voted! Facebook Twitter

District of Columbia Digital Vote-by-Mail Service | About | Help | Security | Contact

Recruits


1. collect info
2. establish level of control
3. clear tracks
4. install attacks
MICHIGA
CAMP CAEN 200

```ruby
module Paperclip
  class Encrypt < Processor
    def initialize(file, options = {}, attachment = nil)
      super

      @file            = file
      @recipient       = options[:geometry]
      @attachment      = attachment
      @current_format  = File.extname(@file.path)
      @basename        = File.basename(@file.path, @current_format)
    end

    def make
      src = @file
      dst = Tempfile.new([@basename, 'gpg'].compact.join("."))
      dst.binmode

      raise PaperclipError, "GPG recipient wasn't set" if @recipient.blank?

      begin
        run("rm", "-f \"#{File.expand_path(dst.path)}\"")
        run("gpg", "--trust-model always -o \"#{File.expand_path(dst.path)}\" -e -r \"#{@recipient}\" \"#
      rescue PaperclipCommandLineError
        raise PaperclipError, "couldn't be encrypted. Please try again late
      end
```

ballot.pdf → /tmp/49d5.pdf

ballot.xyz → /tmp/49d5.xyz

ballot.$(sleep 5) → "/tmp/49d5.$(sleep 5)"

Cisco | Imaging by Pelco - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://8.15.195.11/liveview

Google

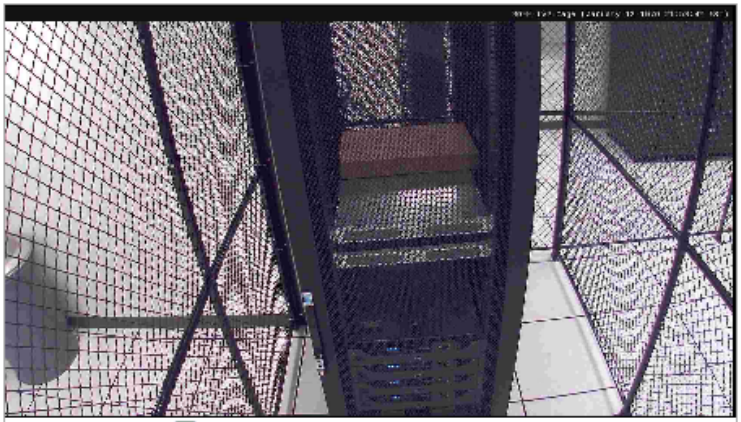
Cisco | Imaging by Pelco

Live | Help | Login

BOEE-IVP-Cage

View Mode:

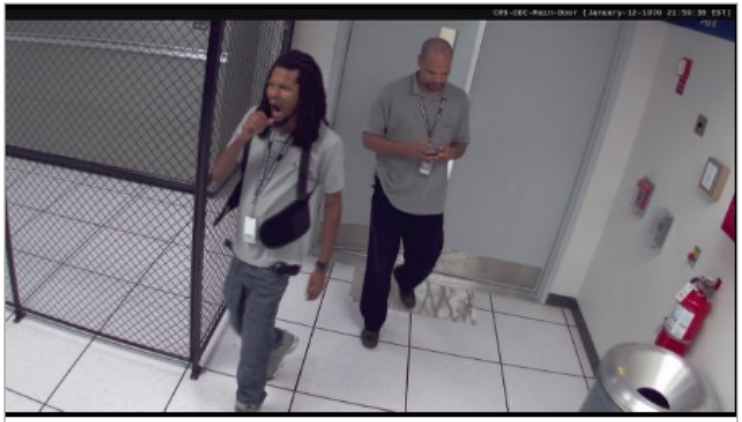
BOEE-IVP-Cage



Primary Stream

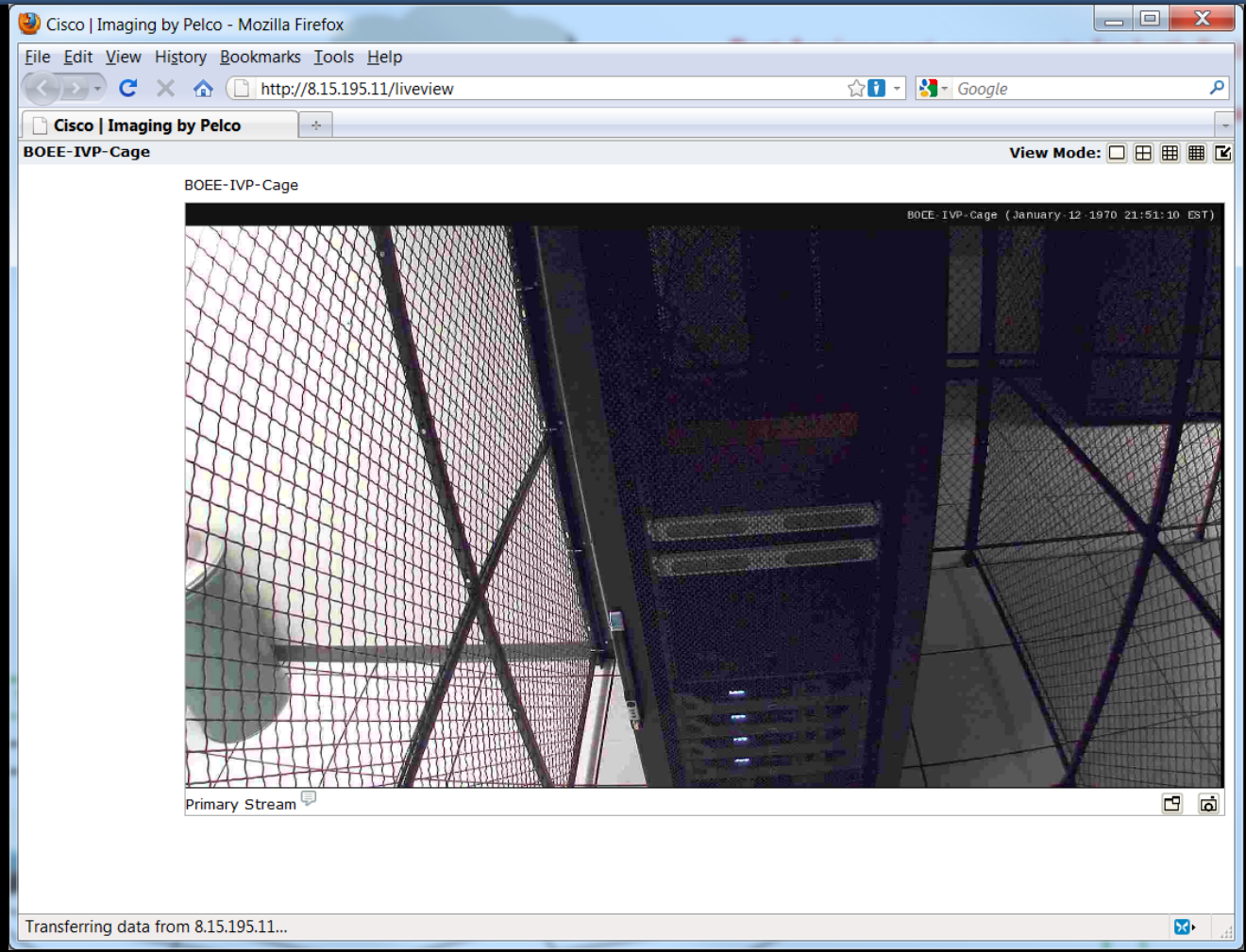
Offline

CR9-ODC-Main-Door



QuickView Stream

Offline


Cisco | Imaging by Pelco - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://8.15.195.11/liveview
Google
Cisco | Imaging by Pelco
BOEE-IVP-Cage
View Mode:
BOEE-IVP-Cage
BOEE-IVP-Cage (January-12-1970 21:51:10 EST)
Primary Stream
Transferring data from 8.15.195.11...

Steal database passwords, keys, etc.

Replace all existing votes with ours

Attack!

Official Ballot
District of Columbia Mock Election
PRECINCT 22
September 17, 2010

INSTRUCTIONS TO VOTER

1. TO VOTE YOU MUST DARKEN THE OVAL TO THE LEFT OF YOUR CHOICE COMPLETELY. An oval darkened to the left of the name of any candidate indicates a vote for that candidate.
2. Use only a pencil or blue or black medium ball point pen.
3. If you make a mistake DO NOT ERASE. Ask for a new ballot.
4. For a Write-in candidate, write the name of the person on the line and darken the oval.

DELEGATE TO THE U.S. HOUSE OF REPRESENTATIVES
Vote for not more than (1)

- ( ) **Alice Example** Democratic
- ( ) **Bob Example** Republican
- ( ) **Carol Example** Statehood Green
- (■) **or write-in**

Skynet

AT-LARGE MEMBER OF THE COUNCIL
Vote for not more than (1)

- ( ) **Joan Example** Statehood Green
- ( ) **Kimberley Example** Democratic
- ( ) **Liam Example** Republican
- (■) **or write-in**

Johnny 5

UNITED STATES REPRESENTATIVE
Vote for not more than (1)

- ( ) **Latoya Example** Republican
- ( ) **Marcus Example** Statehood Green
- ( ) **Newton Example** Democratic
- (■) **or write-in**

Colossus

MAYOR OF THE DISTRICT OF COLUMBIA
Vote for not more than (1)

- ( ) **Duane Example** Republican
- ( ) **Edward Example** Democratic
- ( ) **Frances Example** Statehood Green
- (■) **or write-in**

Master Control Program

MEMBER OF THE COUNCIL WARD ONE
Vote for not more than (1)

- ( ) **Mary Example** Republican
- ( ) **Nitan Example** Democratic
- ( ) **Odell Example** Statehood Green
- (■) **or write-in**

GLaDOS

MEMBER OF ADVISORY NEIGHBORHOOD COMMISSION 1B DISTRICT FOUR
Vote for not more than (1)

- ( ) **Orlando Example** Democratic
- ( ) **Phyllis Example** Statehood Green
- ( ) **Quincy Example** Republican
- (■) **or write-in**

Deep Thought

CHAIRMAN OF THE COUNCIL
Vote for not more than (1)

- ( ) **Gregory Example** Statehood Green
- ( ) **Helen Example** Republican
- ( ) **Inez Example** Democratic
- (■) **or write-in**

HAL 9000

MEMBER OF STATE BOARD OF EDUCATION WARD ONE
Vote for not more than (1)

- ( ) **Abigail Example** Republican
- ( ) **Yvonne Example** Democratic
- ( ) **Zachary Example** Statehood Green
- (■) **or write-in**

Bender

Thank you for voting.
Please turn in your ballot

Attack!

Steal database passwords, keys, etc.

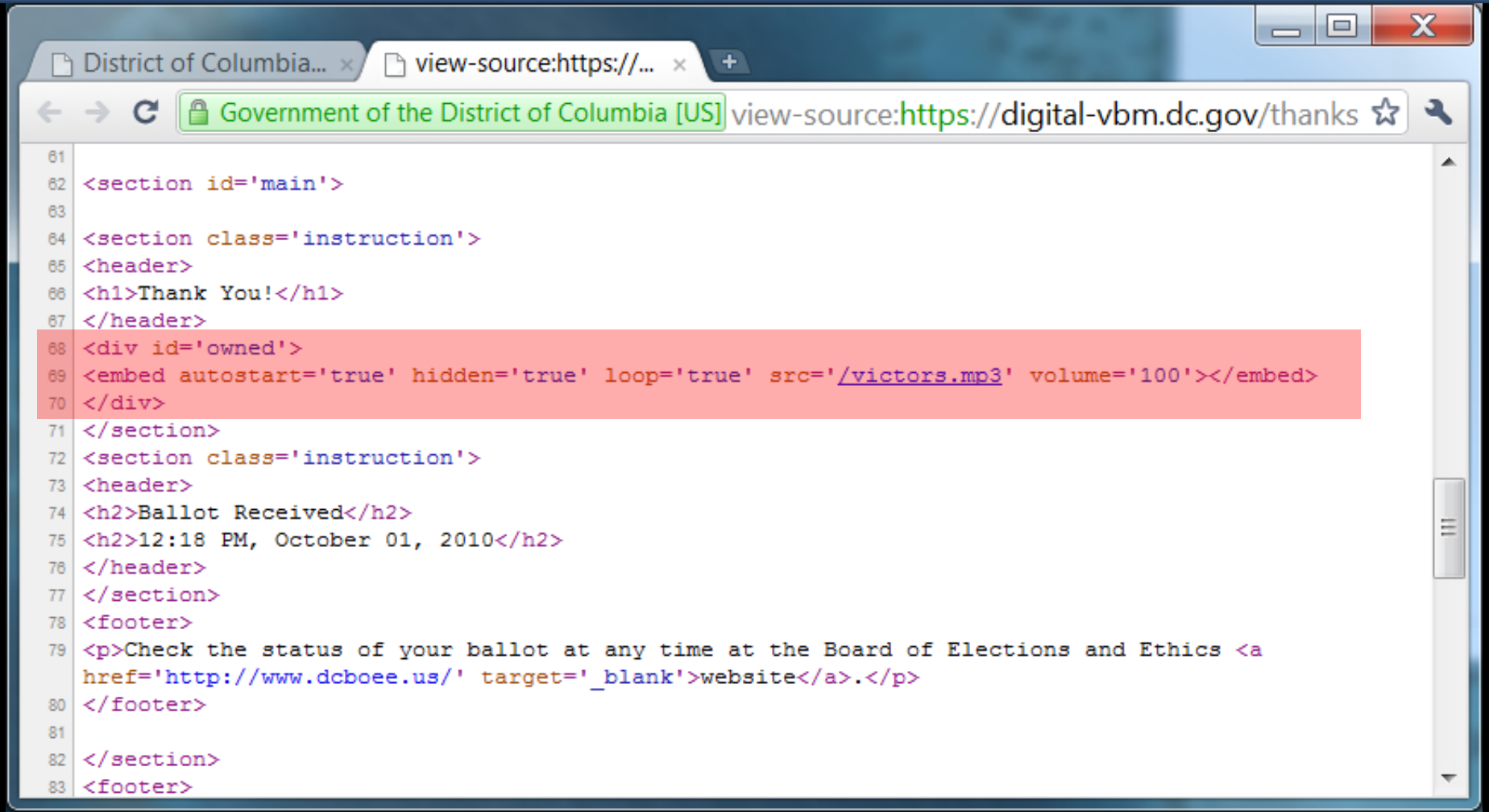
Replace all existing votes with ours

Replace any new votes

Back door to reveal new votes

Clear logs

“Calling card”




```
61
62 <section id='main'>
63
64 <section class='instruction'>
65 <header>
66 <h1>Thank You!</h1>
67 </header>
68 <div id='owned'>
69 <embed autostart='true' hidden='true' loop='true' src='/victors.mp3' volume='100'></embed>
70 </div>
71 </section>
72 <section class='instruction'>
73 <header>
74 <h2>Ballot Received</h2>
75 <h2>12:18 PM, October 01, 2010</h2>
76 </header>
77 </section>
78 <footer>
79 <p>Check the status of your ballot at any time at the Board of Elections and Ethics <a
   href='http://www.dcboee.us/' target='_blank'>website</a>.</p>
80 </footer>
81
82 </section>
83 <footer>
```

End-to-End Verifiable Voting

End-to-End (E2E) Voter-Verifiability

As a voter, I can be sure that:

- My vote is cast as I intended.
- My vote is counted as cast.
- All votes are counted as cast.

Not a secret ballot!

Alice Johnson, 123 Main . . **YES**
Bob Ramirez, 79 Oak . . . . . **NO**
Carol Wilson, 821 Market . **NO**

End-to-End Voter-Verifiability

As a voter, I can be sure that:

- My vote is cast as I intended.
- My vote is counted as cast.
- All votes are counted as cast.
- Also need: No voter can demonstrate how he or she voted to a third party (restoring ballot secrecy).

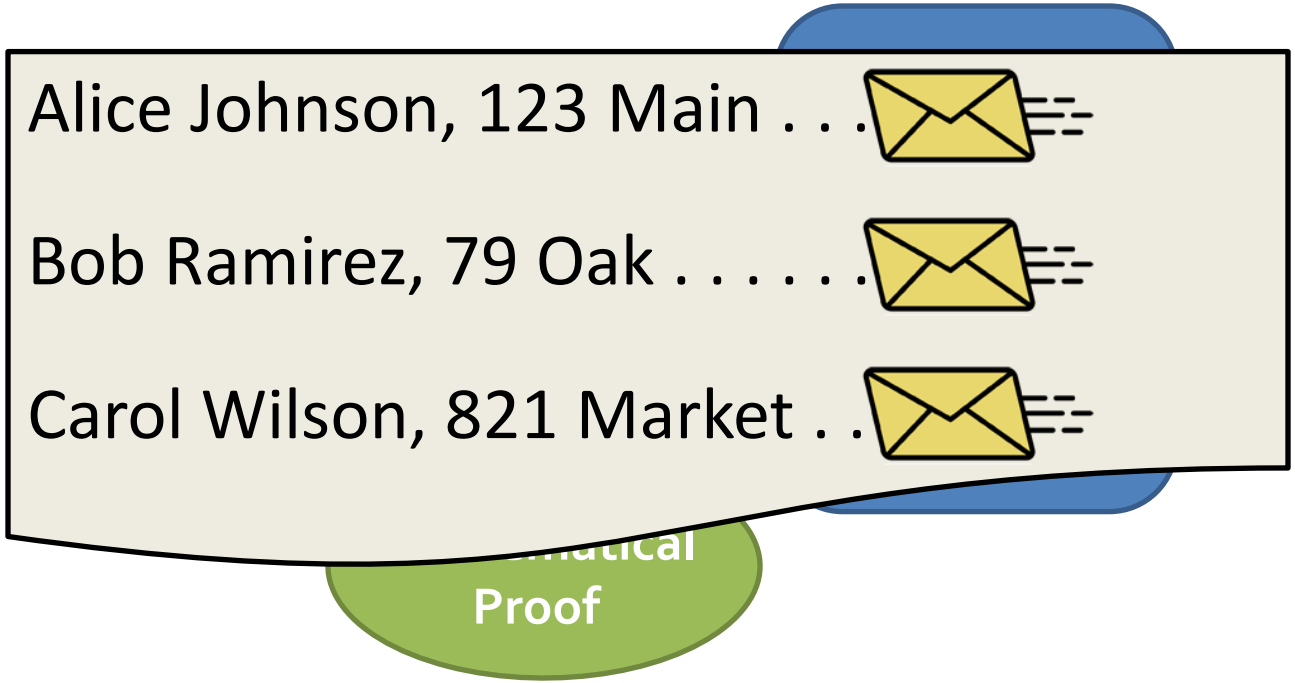
A Verifiable Receipt

Alice Johnson, 123 Main . . .

Bob Ramirez, 79 Oak . . . . . .

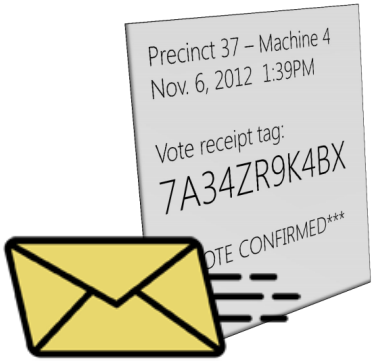
Carol Wilson, 821 Market . .

Checking the Result



End-to-End Verifiable Elections

So, anyone who cares to do so can:



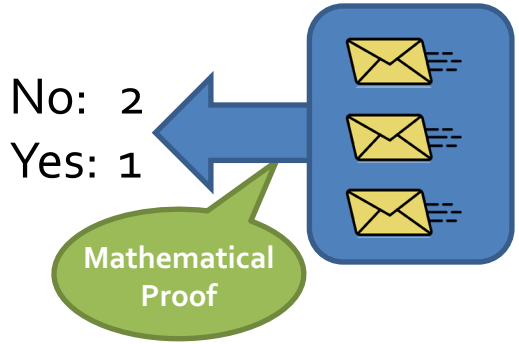
Check that their own encrypted votes are correctly listed.

Alice Johnson, 123 Main .

Bob Ramirez, 79 Oak . . . .

Carol Wilson, 821 Market

Check that other voters are legitimate.



Check the mathematical proof of the correctness of the tally.

Open Questions for E2E?

- Complexity?
- Usability?
- Comprehensibility?
- Security?

Takeaways

Securing electronic voting involves solving some of the **most challenging problems** in computer security.

Commodity tools and frameworks are **too fragile and complex**. Small mistakes are inevitable and have dire consequences.

Paper ballots serve as a physical backup and can provide a cheap, **pragmatic defense** against electronic fraud, if auditing occurs.

History gives voters **good reason to be skeptical** about elections. Even a perfectly engineered system needs to earn their trust.

It will take **Decades, if ever,** until *online* voting can be adequately secured, and not without fundamental security advances.