

EECS 388

# M

# Introduction to Computer Security

Lecture 19:  
**Election Cybersecurity**

November 7, 2023  
Prof. Halderman



# Disinformation about the 2020 Election

Which of these claims is true?

Donald J. Trump @realDonaldTrump

"REPORT: DOMINION DELETED 2.7 MILLION VOTES NATIONWIDE. DATA ANALYSTS SAY PENNSYLVANIA VOTES SWUNG FROM PRESIDENT TRUMP TO BIDEN. OVER 100,000 VOTES DELETED. STATES USING DOMINION VOTING SYSTEMS SWITCHED MILLIONS OF VOTES FROM TRUMP TO BIDEN."

62.1K Quote Tweets 623K Likes

**ZERO CREDIBLE EVIDENCE**

A screenshot of a tweet from Donald J. Trump (@realDonaldTrump). The tweet discusses a report from Dominion regarding the deletion of millions of votes nationwide, specifically mentioning Pennsylvania. It includes a claim that states using Dominion voting systems switched millions of votes from Trump to Biden. A large red diagonal banner across the tweet reads "ZERO CREDIBLE EVIDENCE". Below the tweet are standard social media interaction icons: a speech bubble, a retweet arrow, a heart, and an upward arrow.

BIDEN ADMINISTRATION CORONAVIRUS OPEN SOURCED MORE ▾

## Trump's own officials say he was America's election cheater

Home / Opinion / Trump's own officials say he was America's election cheater

By Vox Staff · 10 hours ago · 10 comments

Trump's own officials say he was America's election cheater

President Donald Trump's claim that millions of votes were deleted from his campaign is not supported by credible evidence, according to several of his own officials who spoke to Vox.

Trump has insisted that millions of votes were deleted from his campaign, particularly in Pennsylvania, where he lost the election by less than 80,000 votes. He has also claimed that millions of votes were added to Biden's total, though there is no evidence to support this claim.

But in recent days, several of Trump's own officials have come forward to say that he was indeed the election cheater.

**HIGHLY MISLEADING**

A screenshot of a Vox article titled "Trump's own officials say he was America's election cheater". The article discusses how several of Trump's own officials have come forward to say that he was indeed the election cheater. A large red diagonal banner across the article reads "HIGHLY MISLEADING". Below the banner is a photograph of several men in suits, likely the officials mentioned in the article, sitting at a table during a press conference.

# The Experts' View

As the National Academies recently concluded, “There is no realistic mechanism to fully secure vote casting and tabulation computer systems from cyber threats.” However, notwithstanding these serious concerns, we have never claimed that technical vulnerabilities have actually been exploited to alter the outcome of any US election.

Anyone asserting that a US election was “rigged” is making an *extraordinary* claim, one that must be supported by persuasive and verifiable evidence. Merely citing the existence of technical flaws does not establish that an attack occurred, much less that it altered an election outcome. It is simply speculation.

The New York Times

## *Election Security Experts Contradict Trump's Voting Claims*

In a public letter, 59 top specialists called the president’s fraud assertions “unsubstantiated” and “technically incoherent.”



By [Nicole Perlroth](#)

Nov. 16, 2020

Fifty-nine of the country’s top computer scientists and election security experts rebuked President Trump’s baseless claims of voter fraud and hacking on Monday, writing that such assertions are “unsubstantiated or are technically incoherent.”

“Anyone asserting that a U.S. election was ‘rigged’ is making an extraordinary claim, one that must be supported by persuasive and verifiable evidence,” the scientists wrote. In the absence of evidence, they added, it is “simply speculation.”

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

# Flashback: Russian Attacks During the 2016 Election

## Targeted political leaks

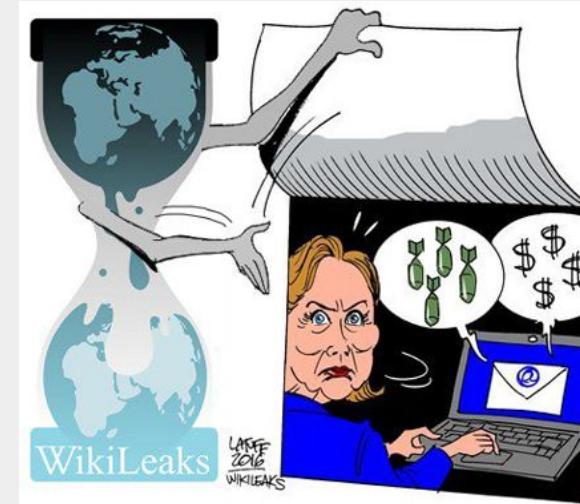
Stolen emails leaked online

## Trolling/message amplification

Goals: Advantage Trump, sow discord

## Attacks on election infrastructure

Registration systems and vendors



**BREAKING**

New Hillary Leaks Series

Wikileaks  
releases  
19,252  
DNC Emails



Shop      Donate

Search



## The Podesta Emails

WikiLeaks series on deals involving Hillary Clinton campaign Chairman John Podesta. Mr Podesta is a long-term associate of the Clintons and was President Bill Clinton's Chief of Staff from 1998 until 2001. Mr Podesta also owns the Podesta Group with his brother Tony, a major lobbying firm and is the Chair of the



The

# Flashback: Russian Attacks During the 2016 Election

## Targeted political leaks

Stolen emails leaked online

## Trolling/message amplification

Goals: Advantage Trump, sow discord

## Attacks on election infrastructure

Registration systems and vendors



A screenshot of a Facebook post from Melvin Redick. The post is titled "BREAKING NEWS - WORLD" and includes a timestamp of June 8, 2016. The main text of the post reads: "These guys show hidden truth about Hillary Clinton, George Soros and other leaders of the US. Visit #DCLeaks website. It's really interesting! <http://dcleaks.com/>". Below the text is a large logo for "DC LEAKS" where the "C" contains a white silhouette of the U.S. Capitol building. At the bottom of the post are standard Facebook interaction buttons for "Like" and "Share", and a small icon indicating one like has been given.

# Flashback: Russian Attacks During the 2016 Election

## Targeted political leaks

Stolen emails published online

## Trolling/message amplification

Goals: Sow discord, advantage Trump

## Attacks on election infrastructure

- All 50 states probed, multiple state voter registration systems infiltrated
- At least one election system vendor infiltrated; attempts to infiltrate county/local election offices
- Attackers had ability to change or destroy registration data (but didn't)
- No evidence that Russia changed votes, but technology didn't stop them

## Report On The Investigation Into Russian Interference In The 2016 Presidential Election

Special Counsel Robert S. Mueller, III

By at least the summer of 2016, GRU officers sought access to state and local computer networks by exploiting known software vulnerabilities on websites of state and local governmental entities. GRU officers, for example, targeted state and local databases of registered voters using a technique known as "SQL injection," by which malicious code was sent to the state or local website in order to run commands (such as exfiltrating the database contents).<sup>188</sup> In one instance in approximately June 2016, the GRU compromised the computer network of the Illinois State Board of Elections by exploiting a vulnerability in the SBOE's website. The GRU then gained access to a database containing information on millions of registered Illinois voters,<sup>189</sup> and extracted data related to thousands of U.S. voters before the malicious activity was identified.<sup>190</sup>

GRU officers **Investigative Technique** scanned state and local websites for vulnerabilities. For example, over a two-day period in July 2016, GRU officers **Investigative Technique** for vulnerabilities on websites of more than two dozen states. **Investigative Technique**

Similar **IT** for vulnerabilities continued through the election.

Unit 74455 also sent spearphishing emails to public officials involved in election administration and personnel at companies involved in voting technology. In August 2016, GRU officers targeted employees of **PP**, a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network. Similarly, in November 2016, the GRU sent spearphishing emails to over 120 email accounts used by Florida county officials responsible for administering the 2016 U.S. election.<sup>191</sup> The spearphishing emails contained an attached Word document coded with malicious software (commonly referred to as a Trojan) that permitted the GRU to access the infected computer.<sup>192</sup> The FBI was separately responsible for this investigation. We understand the FBI believes that this operation enabled the GRU to gain access to the network of at least one Florida county government. The Office did not independently verify that belief and, as explained above, did not undertake the investigative steps that would have been necessary to do so.

# Senate Intelligence Committee Russia Investigation



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

# Integrity

The outcome matches voter intent.

Votes are cast as intended.

Votes are counted as cast.

## 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

Integrity  Ballot Secrecy

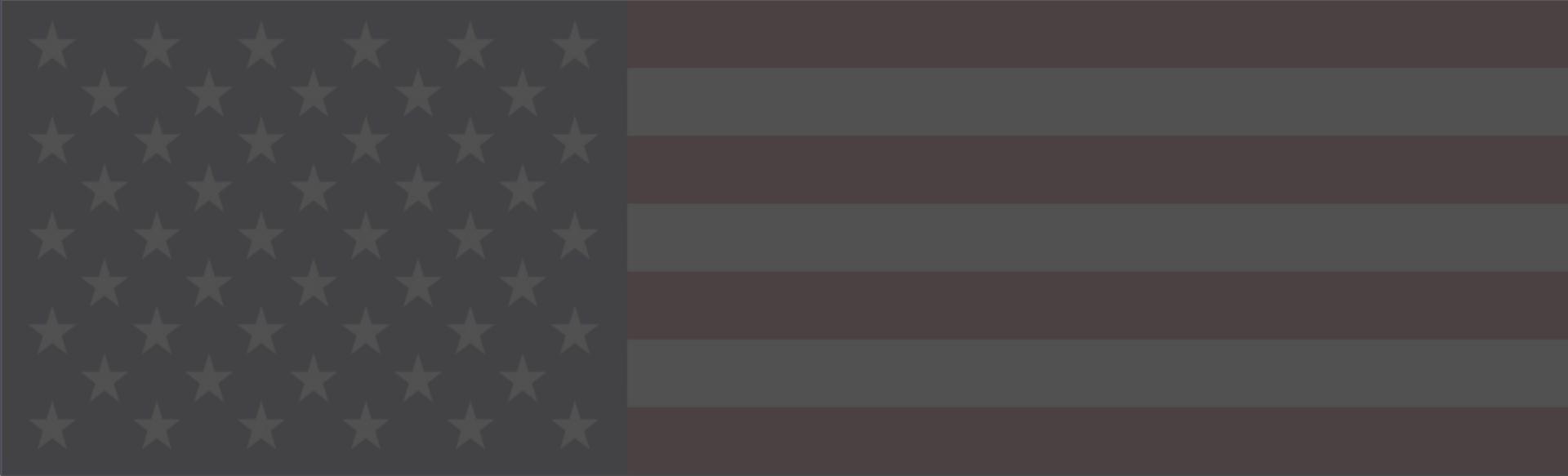
Authentication  Enfranchisement

## Security Requirements

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

## Other Important Properties

- Cost Effectiveness
- Accessibility
- Convenience
- Intelligibility



# Vulnerable Infrastructure

# U.S. Elections

## Scale and Complexity

### Massive Scale

**~170 million** registered voters

### Highly Distributed

State, county, and local levels

**~13,000** voting jurisdictions

**~180,000** election precincts

### Sensitive to Latency

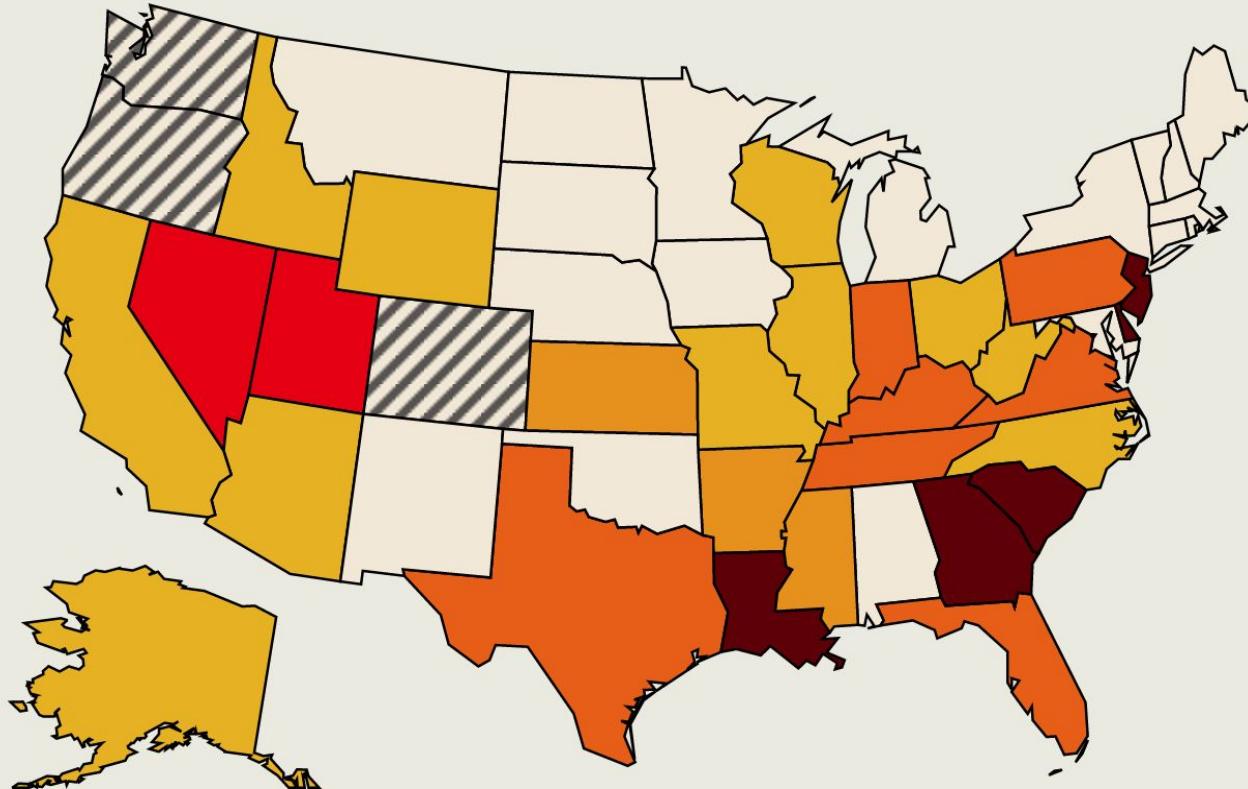
Want results on election night

### High Complexity

Ballots with many different races,  
over a dozen languages, etc.

**~50 models** of voting machines

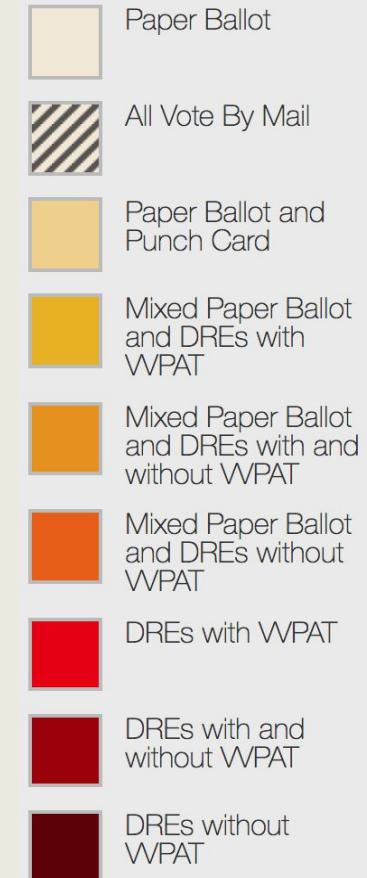
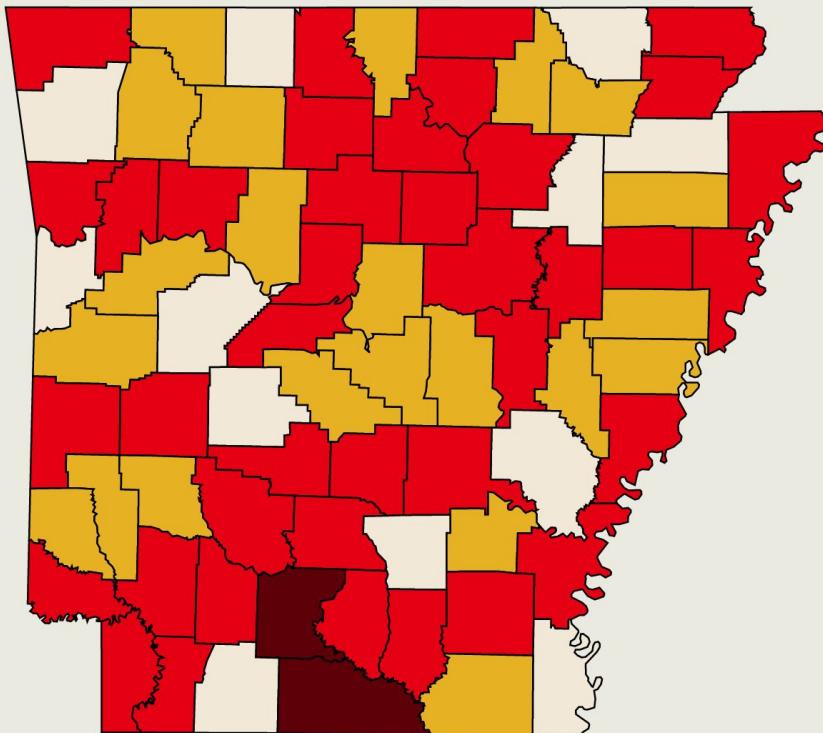
## Election Technology by U.S. State (2016)



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

Data: Verified Voting

## Election Technology by County: State of Arkansas



# U.S. Elections

## November 8, 2016 (8 de noviembre de 2016) Dallas County, Texas (Condado de Dallas, Texas) SAMPLE BALLOT (BOLETA DE MUESTRA)

**INSTRUCTION NOTE:** Vote on the candidate/statement of your choice in each race by darkening in the oval provided to the left of the name of that candidate/statement.

**Straight-Party Vote:** You may cast a straight-party vote (that is, cast a vote for all the nominees of one party) by darkening in the oval provided to the left of the name of the party of your choice. If you cast a straight-party vote for all the nominees of one party and also cast a vote for an opponent of one of that party's nominees, your vote for the opponent will be counted as well as your vote for all the other nominees of the party for which the straight-party vote was cast. Party Abbreviations: Republican Party (Rep); Democratic Party (Dem); Libertarian Party (Lib); Green Party (Grn).

**Voting for a Declared Write-In Candidate:** You may vote for a declared write-in candidate by writing in the name of the candidate on the line provided and darkening in the oval provided to the left of the line.

### USE THE MARKING DEVICE PROVIDED

**NOTA DE INSTRUCCIÓN:** Vote sobre el candidato/declaración de su preferencia en cada compañía electoral al llenar el óvalo provisto a la izquierda del nombre de ese candidato/declaración.

**Voto de Partido Completo:** Usted puede emitir un voto de partido único (es decir, emitir un voto para todos los candidatos de un solo partido) al llenar el óvalo provisto a la izquierda del nombre del partido de su selección. Si usted emite un voto de partido único para todos los nominados de un solo partido y también emite un voto para un oponente de uno de los nominados de ese partido, su voto para el oponente será contado tanto como su voto para todos los demás nominados del partido por el cual fue emitido el voto de partido único. Abreviaturas: Partido Republicano (Rep); Partido Democrático (Dem); Partido Libertario (Lib); Partido Verde (Grn).

**Votando por un Candidato Declarado por Escrito:** Usted puede votar por un candidato declarado por escrito al escribir el nombre del candidato en la línea provista para ese cargo y al llenar el óvalo provisto a la izquierda de la línea.

### UTILICE EL MARCADOR PROPORCIONADO

#### Straight Party (Partido Completo)

##### Republican Party

(Partido Republicano)

##### Democratic Party

(Partido Democrático)

##### Libertarian Party

(Partido Libertario)

##### Green Party

(Partido Verde)

Rep

Dem

Lib

Grn

#### President and Vice President (Presidente y Vice Presidente)

Vote for One (Volar por Uno)

Donald J. Trump / Mike Pence  
Hillary Clinton / Tim Kaine  
Gary Johnson / William Weld  
Jill Stein / Ajamu Baraka

Rep

Dem

Lib

Grn

Write-In (Voto Escrito)

#### United States Representative, District 24 (Representante de los Estados Unidos, Distrito Núm. 24)

Vote for One (Volar por Uno)

Kenny E. Marchant  
Jan McDowell  
Mike Kolls  
Kevin McCormick

Rep  
Dem  
Lib  
Grn

#### United States Representative, District 26 (Representante de los Estados Unidos, Distrito Núm. 26)

Vote for One (Volar por Uno)

Michael C. Burgess  
Eric Mauck  
Mark Boler

Rep  
Dem  
Lib

#### United States Representative, District 30 (Representante de los Estados Unidos, Distrito Núm. 30)

Vote for One (Volar por Uno)

Charles Lingerfelt  
Eddie Bernice Johnson  
Jarrett R. Woods  
Thom Prentice

Rep  
Dem  
Lib  
Grn

#### United States Representative, District 32 (Representante de los Estados Unidos, Distrito Núm. 32)

Vote for One (Volar por Uno)

Pete Sessions  
Ed Rankin

Rep  
Lib

Gary Stuard

Grn

#### United States Representative, District 33 (Representante de los Estados Unidos, Distrito Núm. 33)

Vote for One (Volar por Uno)

M. Mark Mitchell  
Marc Veasey

Rep  
Dem

#### Railroad Commissioner (Comisionado de Ferrocarriles)

Vote for One (Volar por Uno)

Wayne Christian  
Grady Yarbrough  
Mark Miller  
Martina Salinas

Rep  
Dem  
Lib  
Grn

#### Justice, Supreme Court, Place 3 (Juez, Corte Suprema, Lugar Núm. 3)

Vote for One (Volar por Uno)

Debra Lehmann  
Mike Westergren  
Kathie Glass  
Rodolfo Rivera Munoz

Rep  
Dem  
Lib  
Grn

#### Justice, Supreme Court, Place 5 (Juez, Corte Suprema, Lugar Núm. 5)

Vote for One (Volar por Uno)

Paul Green  
Dori Contreras Garza  
Tom Oxford  
Charles E. Waterbury

Rep  
Dem  
Lib  
Grn

#### Justice, Supreme Court, Place 9 (Juez, Corte Suprema, Lugar Núm. 9)

Vote for One (Volar por Uno)

Eva Guzman  
Savannah Robinson  
Don Fulton  
Jim Chisholm

Rep  
Dem  
Lib  
Grn

# Long, Complicated Ballots

United States Representative, Place 2 (Corte de Asambleas, Lugar Núm. 2)  
Vote for One (Volar por Uno)  
Rep  
Dem  
Lib  
Grn

United States Representative, Place 3 (Corte de Asambleas, Lugar Núm. 3)  
Vote for One (Volar por Uno)  
Rep  
Dem  
Lib  
Grn

United States Representative, Place 4 (Corte de Asambleas, Lugar Núm. 4)  
Vote for One (Volar por Uno)  
Rep  
Dem  
Lib  
Grn

United States Representative, Place 5 (Corte de Asambleas, Lugar Núm. 5)  
Vote for One (Volar por Uno)  
Rep  
Dem  
Lib  
Grn

United States Representative, Place 6 (Corte de Asambleas, Lugar Núm. 6)  
Vote for One (Volar por Uno)  
Rep  
Dem  
Lib  
Grn

United States Representative, Place 7 (Corte de Asambleas, Lugar Núm. 7)  
Vote for One (Volar por Uno)  
Rep  
Dem  
Lib  
Grn

United States Representative, Place 8 (Corte de Asambleas, Lugar Núm. 8)  
Vote for One (Volar por Uno)  
Rep  
Dem  
Lib  
Grn

United States Representative, Place 9 (Corte de Asambleas, Lugar Núm. 9)  
Vote for One (Volar por Uno)  
Rep  
Dem  
Lib  
Grn

United States Representative, Place 10 (Corte de Asambleas, Lugar Núm. 10)  
Vote for One (Volar por Uno)  
Rep  
Dem  
Lib  
Grn

United States Representative, Place 11 (Corte de Asambleas, Lugar Núm. 11)  
Vote for One (Volar por Uno)  
Rep  
Dem  
Lib  
Grn

United States Representative, Place 12 (Corte de Asambleas, Lugar Núm. 12)  
Vote for One (Volar por Uno)  
Rep  
Dem  
Lib  
Grn

United States Representative, Place 13 (Corte de Asambleas, Lugar Núm. 13)  
Vote for One (Volar por Uno)  
Rep  
Dem  
Lib  
Grn

United States Representative, Place 14 (Corte de Asambleas, Lugar Núm. 14)  
Vote for One (Volar por Uno)  
Rep  
Dem  
Lib  
Grn

United States Representative, Place 15 (Corte de Asambleas, Lugar Núm. 15)  
Vote for One (Volar por Uno)  
Rep  
Dem  
Lib  
Grn

United States Representative, Place 16 (Corte de Asambleas, Lugar Núm. 16)  
Vote for One (Volar por Uno)  
Rep  
Dem  
Lib  
Grn

United States Representative, Place 17 (Corte de Asambleas, Lugar Núm. 17)  
Vote for One (Volar por Uno)  
Rep  
Dem  
Lib  
Grn

# U.S. Voting Machines

3 main styles, chosen by state/locality



## Hand-Marked Optical Scan

Computer counts hand-marked ballots received by mail or as they're deposited in a ballot box



## BMD (Ballot Marking Device)

Votes cast on screen, printed on paper, counted by optical scanner.  
Widely used for accessibility



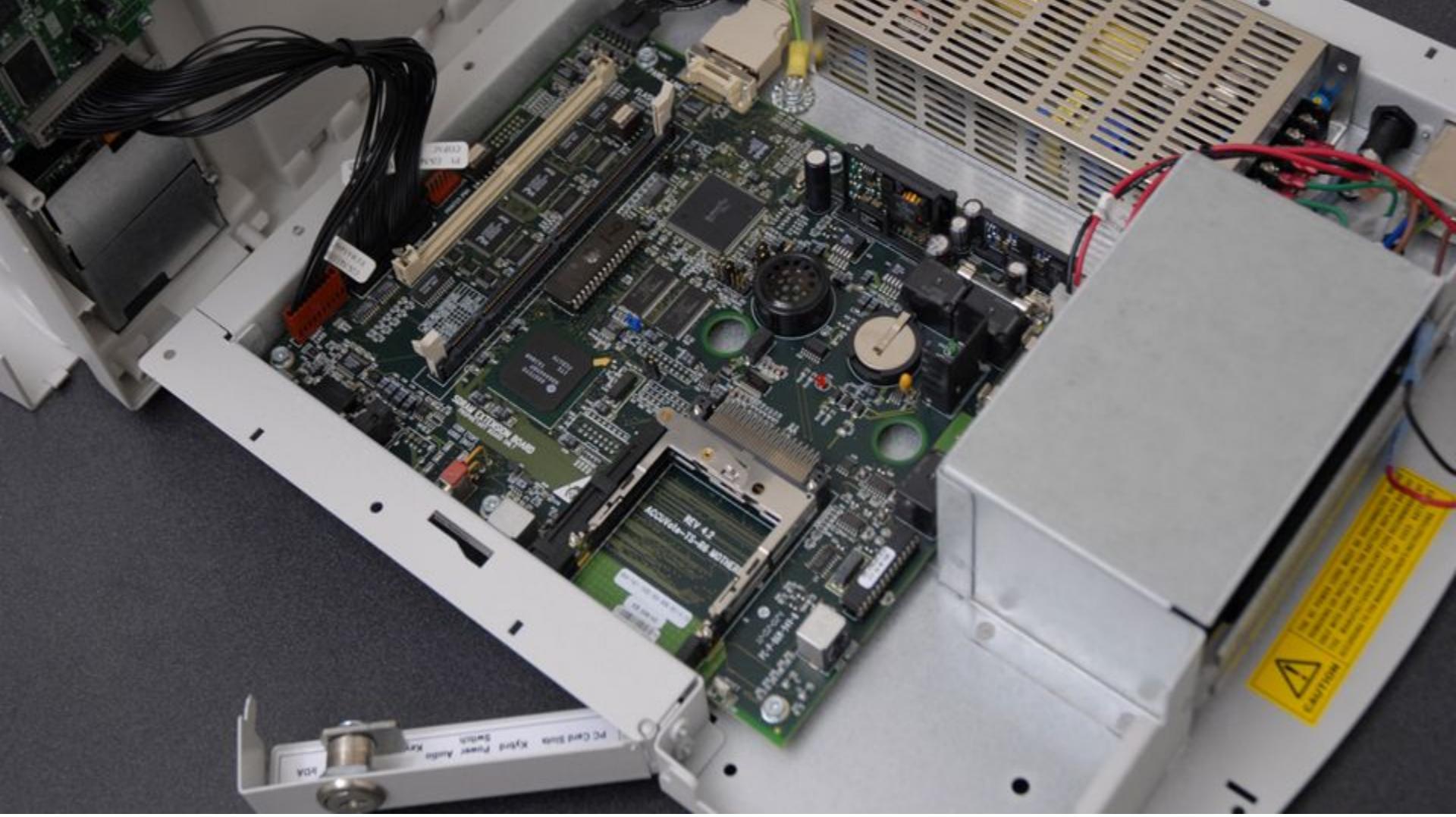
## DRE (Direct-Recording Electronic)

Votes cast on screen, recorded in memory. Some models also print a paper audit trail (VVPAT)

# Are U.S. Voting Machines Secure?



AccuVote TS-X





1. Attacker infects memory card containing ballot programming files.

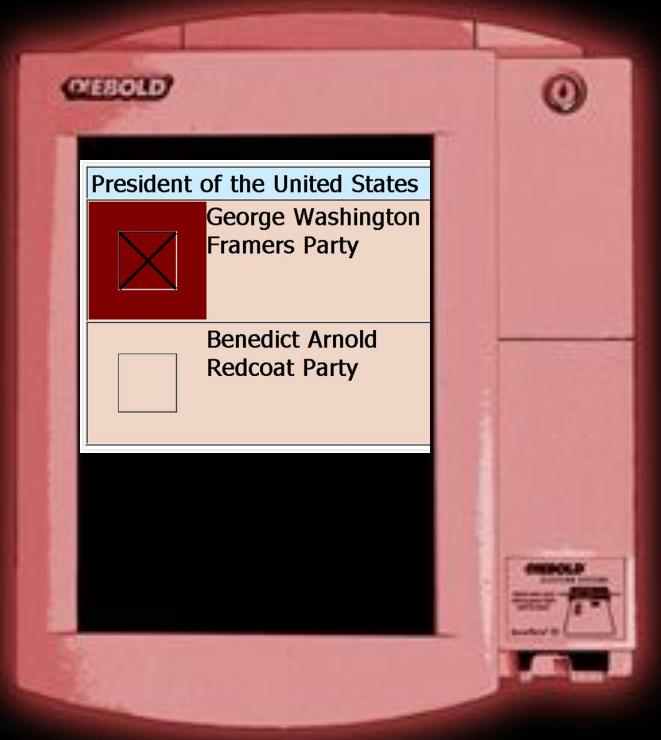




2. When officials place the card into the machine, it becomes infected.

AccuVote TS-X can be infected through:

- Unauthenticated **software update** mechanism;
- **Buffer overflows** in code that reads ballot design; or
- **Interpreted programming language** (AccuBasic) used to print result tape.



3. Malware running on the machine can arbitrarily change electronic records and printouts.

```
*****
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
```

# Pervasive Security Problems

## Source Code Review of the Diebold Voting System (2007)

Calandrino, Feldman, Halderman, Wagner, Yu, and Zeller

Part of the California Secretary of State's "Top-to-Bottom" Voting System Review.

5.2.1 The AV-TSX automatically installs bootloader and operating system updates from the memory card without verifying the authenticity

5.2.2 The AV-TSX automatically installs application updates from the memory card without verifying the authenticity

5.2.3 Multiple buffer overflows allow arbitrary code execution on startup

5.2.4 Setting a jumper enables a bootloader menu that allows the user to extract or tamper with the contents of the internal flash memory

5.2.5 Keys used to secure election data are not adequately protected

5.2.6 Malicious code running on the machine could manipulate election databases, results, and audit logs

5.2.7 The smart card authentication protocol can be broken, providing access to administrator functions and the ability to cast multiple votes

5.2.8 Security key cards can be forged and used to change system keys

5.2.9 A local user can get to the Setup menu without a smart card or key

5.2.10 The protective counter is subject to tampering

5.2.11 SSL certificates used to authenticate can be stolen and have an obvious password

5.2.12 OpenSSL is not initialized with adequate entropy

5.2.13 Multiple vulnerabilities in the AccuBasic interpreter allow arbitrary code execution

5.2.14 Tampering with the memory card can result in code execution during voting

5.2.15 A malicious election file on the memory card could exploit multiple vulnerabilities to run arbitrary code

5.2.16 Malicious election files can cause arbitrary code execution on the AV-TSX when uploading elections

5.2.17 A buffer overflow in the handling of IP addresses might be exploitable by voters

5.2.22 Files on the voting machine are not securely erased when they are deleted

5.2.23 Logic errors may create a vulnerability when displaying bootloader bitmap images

5.2.24 AV-TSX startup code contains blatant errors

# Every U.S. voting machine subjected to rigorous independent security review suffered vulnerabilities that would enable vote-altering attacks



**Hart InterCivic eSlate**  
Cards spread malware (2007)



**AVC Advantage**  
Cards spread malware (2009)



**Sequoia AVC Edge**  
Cards spread malware (2007)



**Optech Insight**  
Cards spread malware (2007)



**ES&S iVotronic**  
Cards spread malware (2007)



**Diebold AccuVote TSX**  
Cards spread malware (2007)



**Diebold AccuVote OS**  
Cards spread malware (2007)



**Dominion ICX BMD**  
Cards spread malware (2021)

# Are More Recent Voting Machines More Secure?



CYBERSECURITY  
& INFRASTRUCTURE  
SECURITY AGENCY



Alerts and Tips

Resources

ICS-CERT Advisories > Vulnerabilities Affecting Dominion Voting Systems ImageCast X

## ICS Advisory (ICSA-22-154-01)

### Vulnerabilities Affecting Dominion Voting Systems ImageCast X

Original release date: June 03, 2022

## 2.4 RESEARCHER

J. Alex Halderman, University of Michigan, and Drew Springall, Auburn University

June 2022:  
CISA's first-ever advisory  
about election  
equipment vulnerabilities

IMAGECAST<sup>®</sup> X | BMD



Get in touch  
1866.654.VOTE (8683)  
sales@dominionvoting.com  
www.dominionvoting.com

DOMINION  
VOTING

# Viral Malware Installation

## 2.2.1 IMPROPER VERIFICATION OF CRYPTOGRAPHIC SIGNATURE CWE-347



The tested version of ImageCast X does not validate application signatures to a trusted root certificate. Use of a trusted root certificate ensures software installed on a device is traceable to, or verifiable against, a cryptographic key provided by the manufacturer to detect tampering. An attacker could leverage this vulnerability to install malicious code, which could also be spread to other vulnerable ImageCast X devices via removable media.

## 2.2.5 PATH TRAVERSAL: './FILEDIR' CWE-24



The tested version of ImageCast X can be manipulated to cause arbitrary code execution by specially crafted election definition files. An attacker could leverage this vulnerability to spread malicious code to ImageCast X devices from the EMS.

## 2.2.6 EXECUTION WITH UNNECESSARY PRIVILEGES CWE-250

```
# whoami  
root
```

Applications on the tested version of ImageCast X can execute code with elevated privileges by exploiting a system level service. An attacker could leverage this vulnerability to escalate privileges on a device and/or install malicious code.

# Serious Privacy Vulnerability



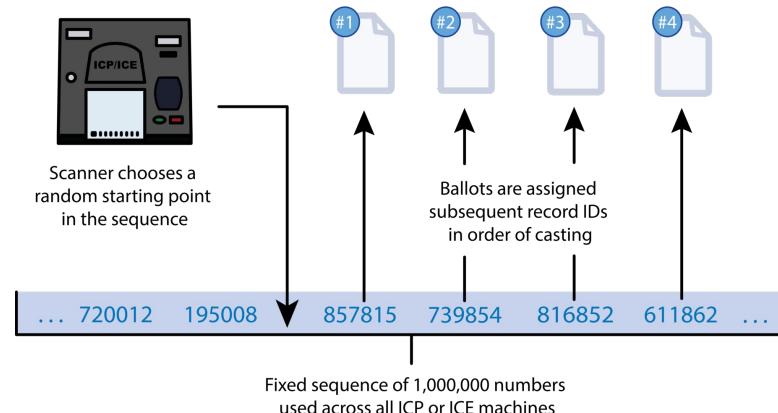
## Cast Vote Records (CVRs)

Often treated as public records

TabulatorNum	BatchId	RecordId	CountingGroup	PrecinctPortion
987	0	546984	Election Day	City of Detroit, P
987	0	749347	Election Day	City of Detroit, P
987	0	299063	Election Day	City of Detroit, P
987	0	607574	Election Day	City of Detroit, P

## Dominion ICP and ICE Scanners

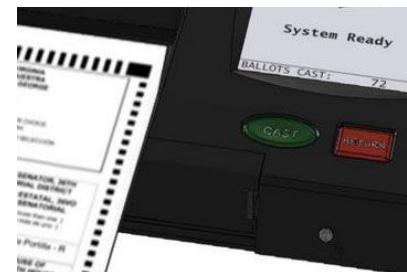
(Used in parts of 21 states)



PRNG is just a lightly-obfuscated linear congruent generator (LCG)!  
Used in parts of 21 states

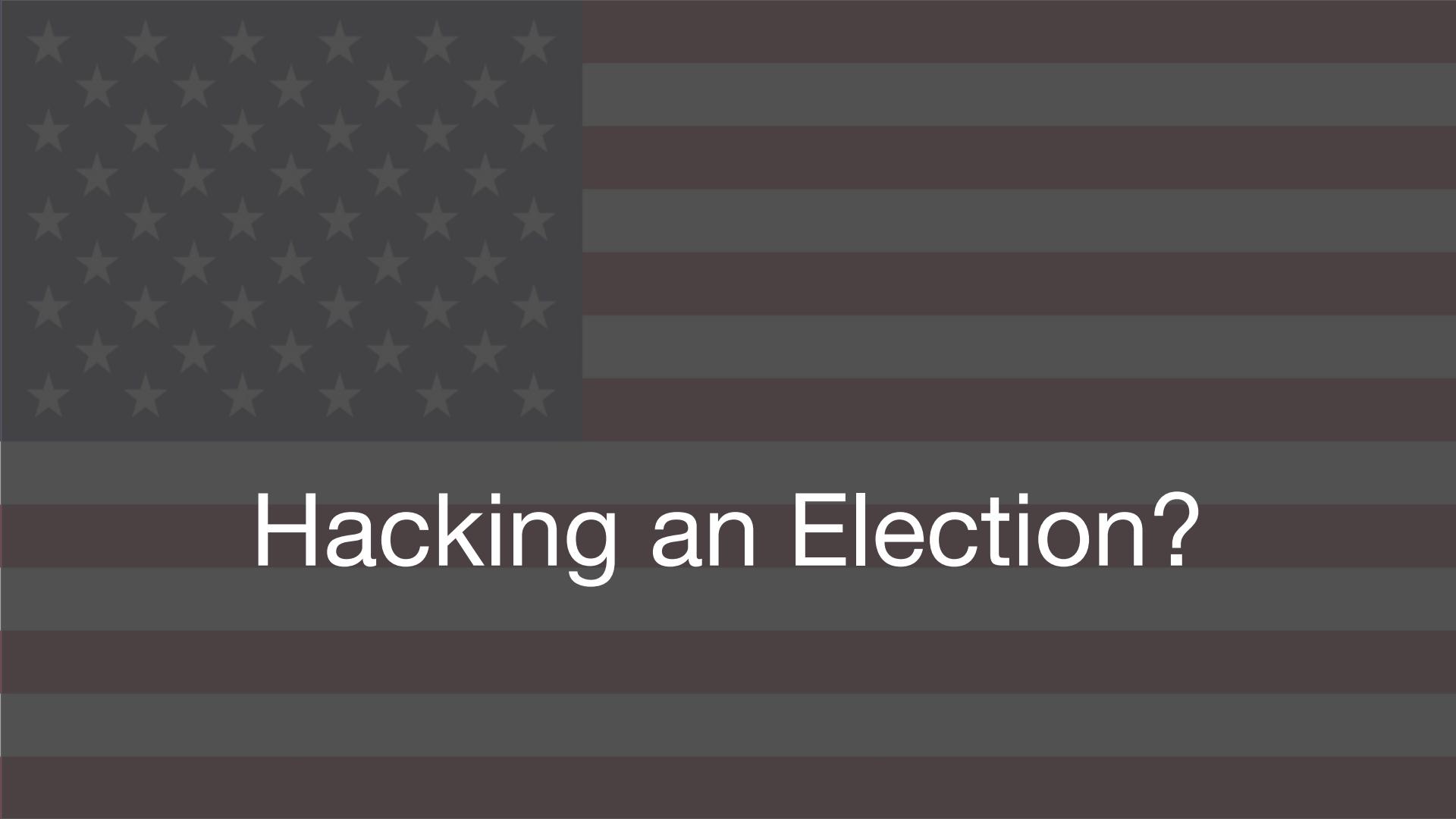
```
def generate_sequence(p):  
    return [sum([5,0,8,3,2,6,1,9,4,7][864803*n//10**p[i]%10]*10**i  
              for i in range(6)) for n in range(1000000)]  
  
icp_sequence = generate_sequence([2,3,1,5,0,4])
```

Anyone can note  
Public Counter



Some localities:  
All-day video footage!





# Hacking an Election?

# Cyberattacks on Election Infrastructure

## Altering election-night results

Detectable, but undermines credibility

## Sabotage registration/poll books

Selectively cause long lines, etc.

## Manipulating voting machines

Potential for *invisible* outcome changes

The screenshot shows a news article from The Christian Science Monitor. The header features the publication's name in a large serif font, with "The CHRISTIAN SCIENCE" in smaller letters above "MONITOR". Below the name are links for "Log In" and "Register", and a link for "FREE E-mail Newsletters". The main headline is "Ukraine election narrowly avoided 'wanton destruction' from hackers". The sub-headline reads: "A brazen three-pronged cyber-attack against last month's Ukrainian presidential elections has set the world on notice – and bears Russian fingerprints, some say." The author is listed as "By Mark Clayton, Staff writer" and the date is "JUNE 17, 2014". A "Save for later" button is visible. The main body of the article discusses a three-pronged cyber-attack on Ukraine's presidential election, mentioning fake computer vote totals and government cyber experts.

WORLD | PASSCODE

## Ukraine election narrowly avoided 'wanton destruction' from hackers

A brazen three-pronged cyber-attack against last month's Ukrainian presidential elections has set the world on notice – and bears Russian fingerprints, some say.

By Mark Clayton, Staff writer ▾ | JUNE 17, 2014

Save for later

A three-pronged wave of cyber-attacks aimed at wrecking Ukraine's presidential vote – including an attempt to fake computer vote totals – was narrowly defeated by government cyber experts, Ukrainian officials say.

The still little-known hacks, which surfaced May 22-26, appear to be among the most dangerous cyber-attacks yet deployed to sabotage a national election – and a warning shot for future elections in the US and abroad, political scientists and cyber experts say.

# Cyberattacks on Election Infrastructure

## Altering election-night results

Detectable, but undermines credibility

## Sabotage registration/poll books

Selectively cause long lines, etc.

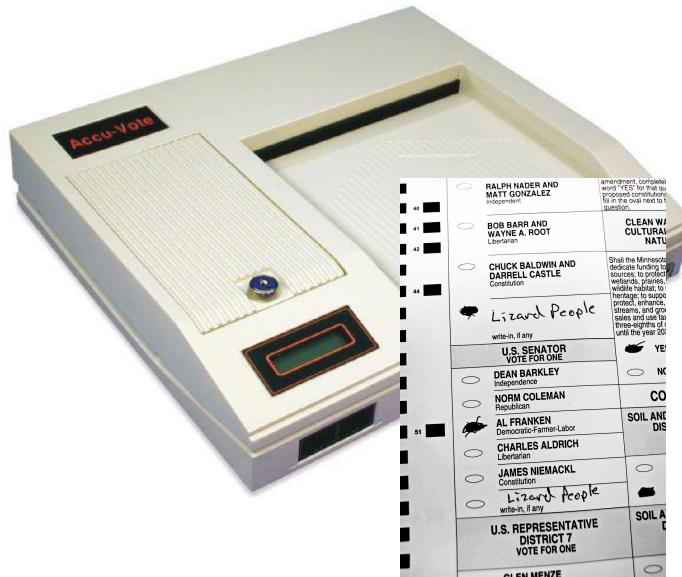
## Manipulating voting machines

Potential for *invisible* outcome changes

# Election Hacking

# Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?



## Challenge 1

Diverse, decentralized voting technology

## Challenge 2

Machines aren't connected to the Internet

## Challenge 3

>85% of U.S. votes have a paper record

# Election Hacking

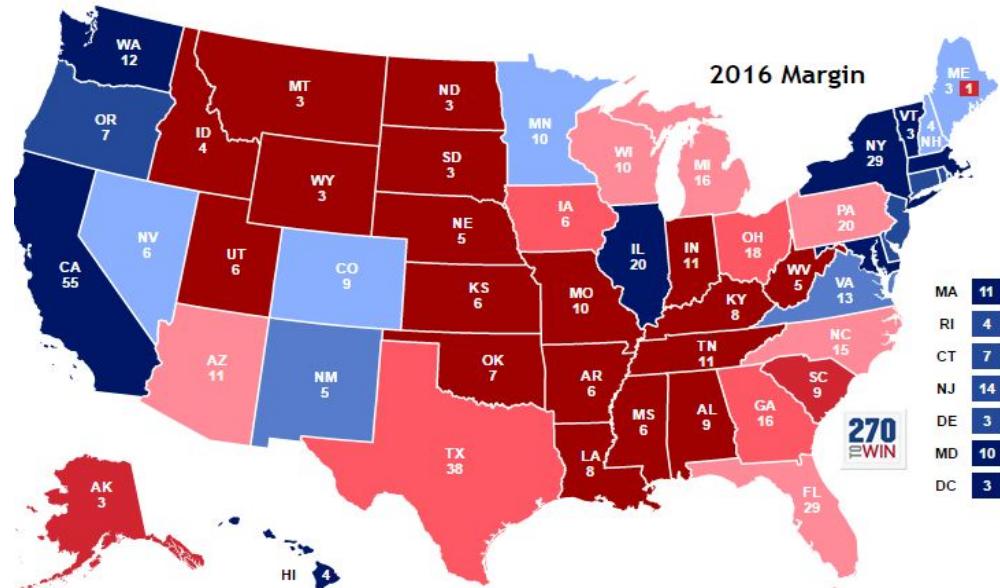
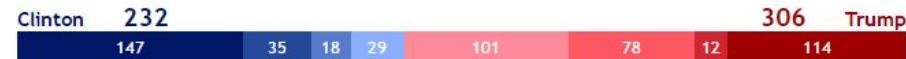
How hard would it be to invisibly change a national election outcome, by tampering with voting machines?



# Invisible Attacks

## Challenge 1

Diverse, decentralized voting technology



# Election Hacking

# Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?



## Challenge 1

~~Diverse, decentralized voting technology~~  
**Choose weakest targets in closest states.**

## Challenge 2

Machines aren't connected to the Internet

## Challenge 3

>85% of U.S. votes have a paper record

# Election Hacking

# Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?



## Challenge 1

~~Diverse, decentralized voting technology~~  
**Choose weakest targets in closest states.**

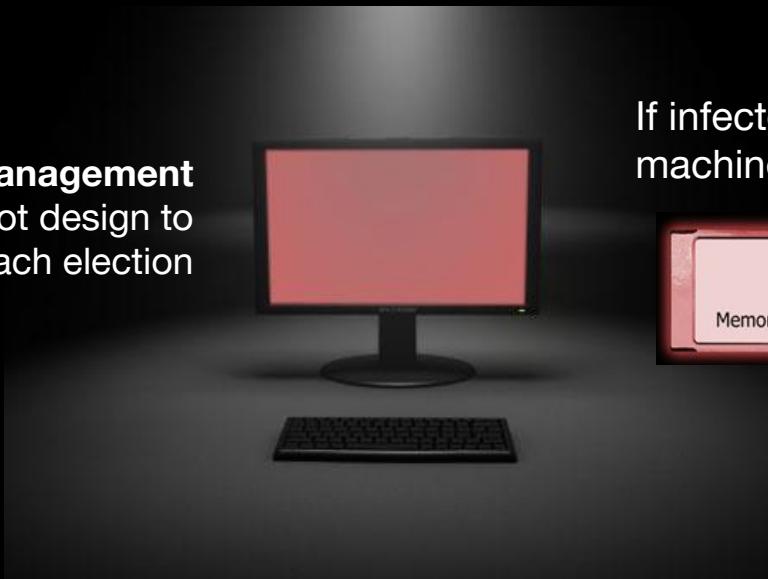
## Challenge 2

Machines aren't connected to the Internet

## Challenge 3

>85% of U.S. votes have a paper record

Centralized **election management computer** programs ballot design to memory cards before each election



If infected, can spread malware to all machines across one or more counties

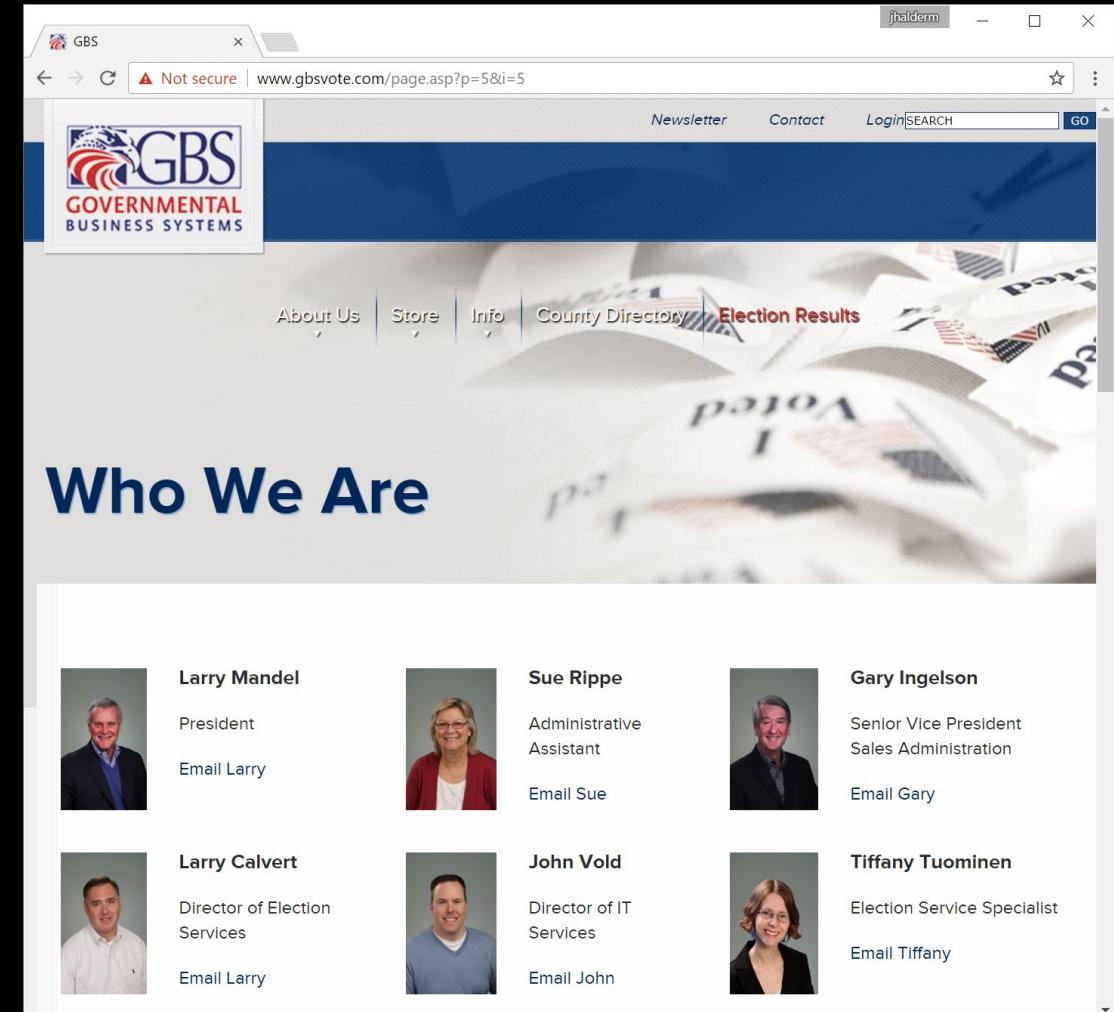




How hard would it be  
to attack an election  
management computer?

Many jurisdictions outsource  
their ballot programming  
to small, outside businesses.

75% of Michigan counties use  
just two ~20 person companies.



The screenshot shows a web browser window for the GBS (Governmental Business Systems) website at [www.gbsvote.com/page.asp?p=5&i=5](http://www.gbsvote.com/page.asp?p=5&i=5). The page title is "Who We Are". The header includes the GBS logo, navigation links for Newsletter, Contact, Login, and a search bar, and a "GO" button. Below the header is a banner image of a ballot box. The main content area features six staff profiles arranged in a grid:

Profile Picture	Name	Title	Contact Information
	Larry Mandel	President	Email Larry
	Sue Rippe	Administrative Assistant	Email Sue
	Gary Ingelson	Senior Vice President Sales Administration	Email Gary
	Larry Calvert	Director of Election Services	Email Larry
	John Vold	Director of IT Services	Email John
	Tiffany Tuominen	Election Service Specialist	Email Tiffany



How hard would it be  
to attack an election  
management computer?

## Growing threat: Politically motivated insiders

# Video appears to undercut Trump elector's account of alleged voting-data breach in Georgia

By Jon Swaine and Emma Brown

Updated September 20, 2022 at 1:04 a.m. EDT | Published September 20, 2022 at 12:00 a.m. EDT



On Jan. 7, 2021, a group of forensics experts working for lawyers allied with President Donald Trump spent eight hours at a county elections office in southern Georgia, copying sensitive software and data from its voting machines.

# Election Hacking

# Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?



## Challenge 1

~~Diverse, decentralized voting technology~~  
Choose weakest targets in closest states.

## Challenge 2

~~Machines aren't connected to the Internet~~  
Target election management computers  
to spread malware to the voting machines.

## Challenge 3

>85% of U.S. votes have a paper record

# Election Hacking

# Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?



## Challenge 1

~~Diverse, decentralized voting technology~~  
Choose weakest targets in closest states.

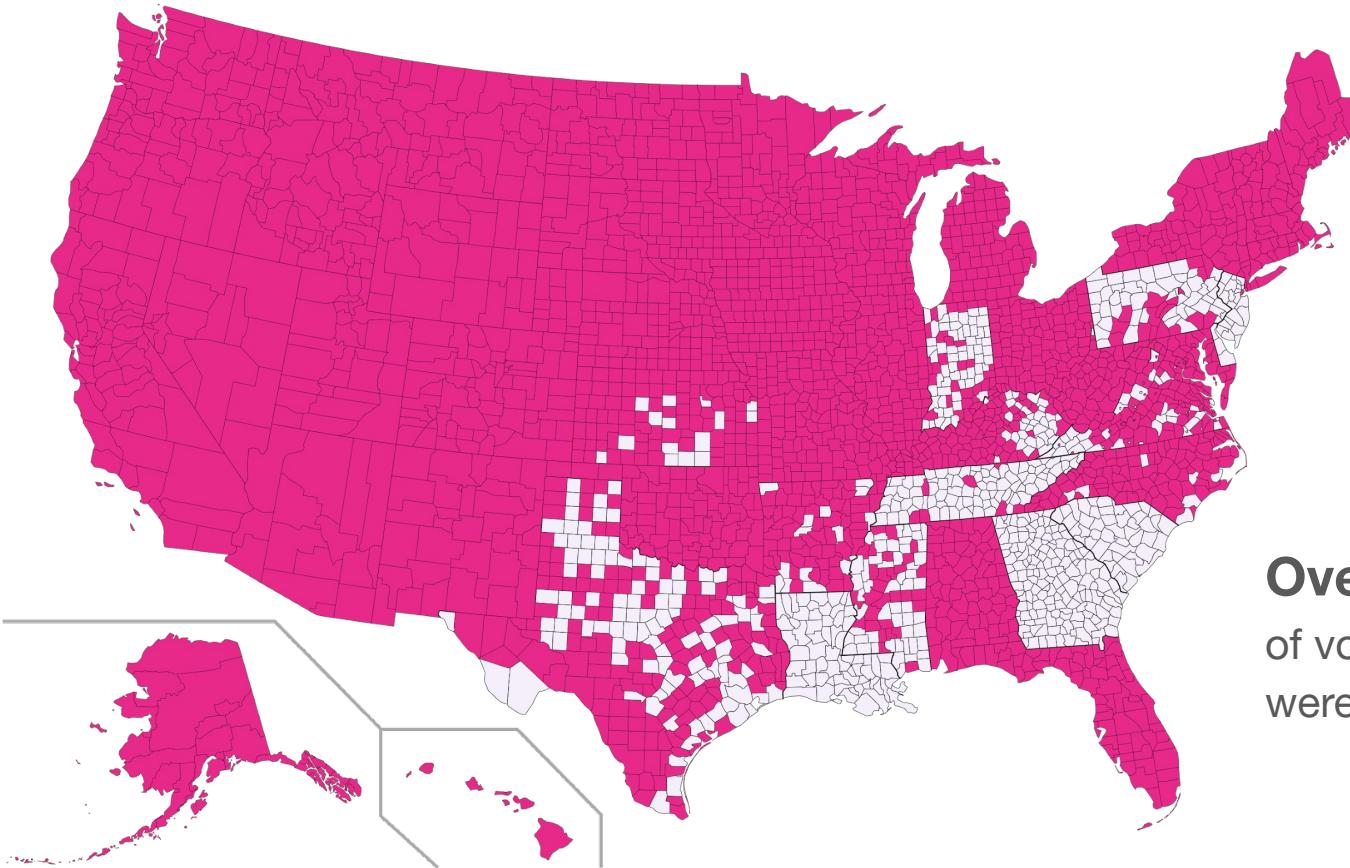
## Challenge 2

~~Machines aren't connected to the Internet~~  
Target election management computers  
to spread malware to the voting machines.

## Challenge 3

>85% of U.S. votes have a paper record

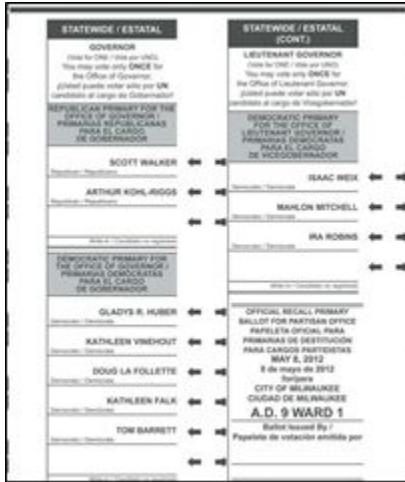
# Use of Paper has Increased



**Over 85%**  
of votes cast in 2020  
were recorded on paper.



# Paper as a Defense



Slow/expensive to tally  
**Verified by voter**

Fast/cheap to tally  
Unverified

# Paper as a Defense



## Risk-Limiting Audit (RLA)

**Hand count *enough* paper ballots** to ensure that, if the reported outcome is wrong, then the audit has a high probability of detecting the discrepancy

Provides strong *affirmative evidence* that the election outcome is correct

National Academies recommend states adopt RLAs by 2028 for all federal/statewide contests

# Election Hacking

# Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?



## Challenge 1

~~Diverse, decentralized voting technology~~  
Choose weakest targets in closest states.

## Challenge 2

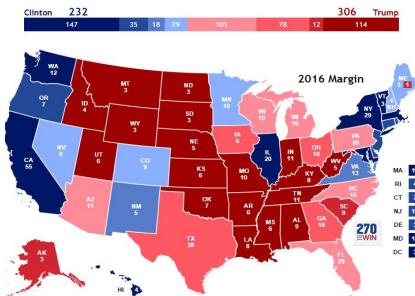
~~Machines aren't connected to the Internet~~  
Target election management computers  
to spread malware to the voting machines.

## Challenge 3

~~85% of U.S. votes have a paper record~~  
**Most states won't look at the paper!**

# Election Hacking

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?



## Step 1

Use pre-election polls to identify likely close states, choose weakest targets.

## Step 2

Target jurisdictions or service providers, and compromise election management computers.

# Invisible Attacks

**Far from easy,  
but within reach for  
sophisticated attackers**



Sue Rippe  
Administrative Assistant  
Email Sue



## Step 3

Infected memory cards exploit vulnerable voting machines to run malware, swap, e.g., 2% of votes.

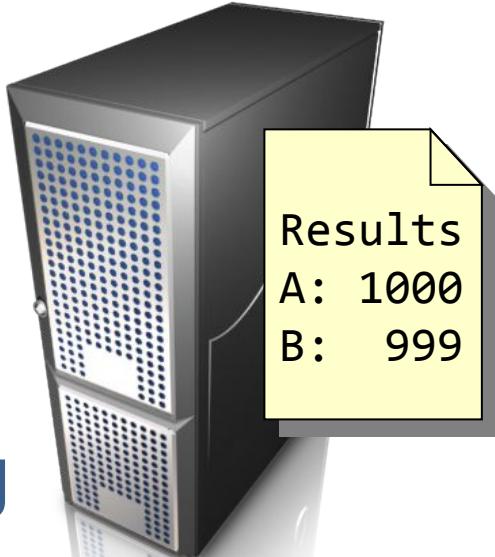
## Step 4

Most states will throw away the ballots without rigorously checking.



# Internet Voting?!

# Server-side threats to online voting



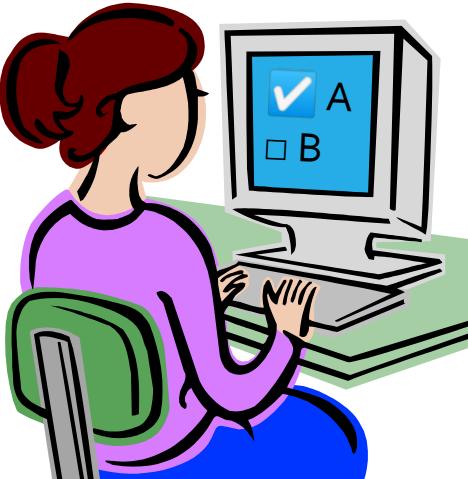
Remote Intrusion

Insider Attacks

Supply-chain Attacks

Denial of Service

# Client-side threats to online voting

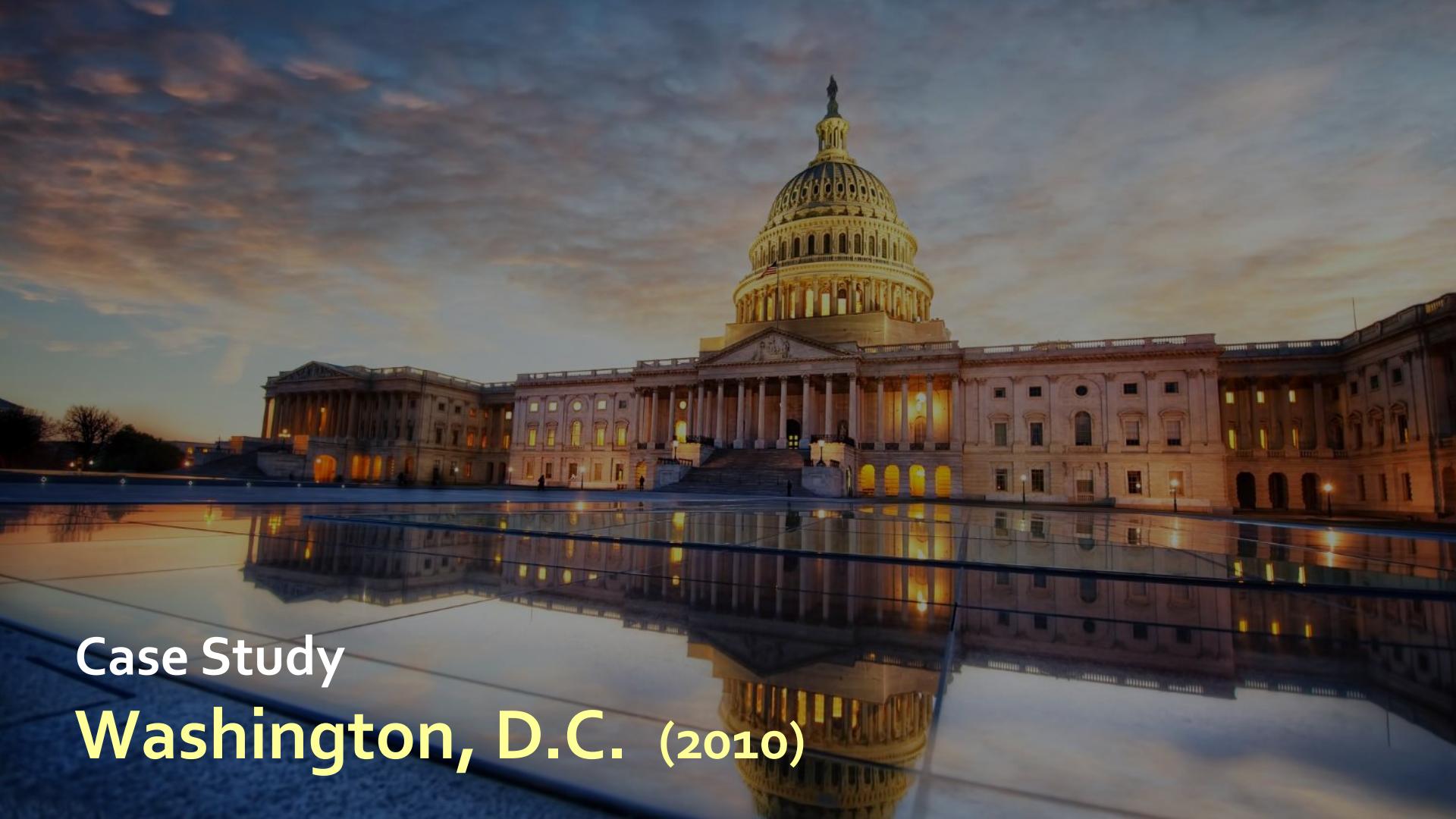


Coercion

Malware / Bots

Credential Theft

Imposter Sites



# Case Study Washington, D.C. (2010)



DC Specific Election  
November 2, 2010

#### Digital Vote-by-Mail Service

Here are the steps you will follow to complete your ballot. Once you have reviewed the steps, click Continue.

1

## Check In

Enter name, ZIP code, voter ID number, and PIN

2

## Confirm Identity

Confirm your identity  
Affirm voting eligibility  
Review attestation document (optional)

3

## Complete Ballot

Download your ballot  
View your ballot  
Mark your ballot  
Save your ballot (Do NOT rename the file.)

4

## Send Ballot

Locate your ballot on your computer  
Upload your ballot  
Receive notice of ballot receipt

[Back](#)

[Continue](#)

#### Key Dates

**October 1**

Vote-by-Mail service begins

**October 22**

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

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

# 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](mailto: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.

Digital Vote by Mail is a first-in-the-nation use of open source technology to provide a secure means for overseas voters to obtain, print and mail their ballot...and, if the voter



# DC General Election

## November 2, 2010

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.

---

**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.

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*

[Start Mail-in Ballot](#)

[Start Digital Ballot](#)



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

**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

# 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](#)

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.



DC Specific Election  
November 2, 2010

#### Confirm Your Identity

To vote through the Digital-Vote-by-Mail Service, you must confirm your identity and your eligibility to vote. Select the checkboxes to confirm. You can also review the attestation document that confirms your voting eligibility by clicking on the PDF. (This step is optional.) [Keep this page open until you have finished viewing your attestation document.](#)

1 Check In

2 Confirm Identity

3 Complete Ballot

4 Send Ballot

## Confirm

#### Confirm Your Identity

Please confirm your identity and voter registration address. If the address shown is incorrect, you will need to contact the BOEE to have it updated before you can mark your ballot. If the information is correct, check the box.

If this isn't you, press the Back button and re-enter your information.

Iva Pfannerstill  
Addison Ave, Unit 261  
WASHINGTON DC 20018



Check the box to certify that you are the person indicated.

## Affirm

#### Affirm Your Eligibility

Review the text inline. Check the box to confirm statements are correct.

I swear or affirm, under penalty of perjury, that:

1. I am a U.S. citizen, at least 18 years of age, and I am eligible to vote in the District of Columbia; and



By checking the box above, I affirm that the information on this form is true, accurate, and complete to the best of my knowledge, and that I understand that a material misstatement of fact in completion of this document may constitute grounds for a conviction for perjury.

## Review

#### Review Your Attestation Document (Optional Step)

If you would like to review your attestation document, click the PDF icon at the right. The document will open in your default PDF viewing application, or tap it if you are using a mobile device.



Open  
Attestation



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

#### 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

# 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

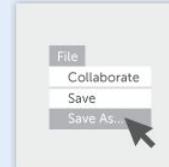
To complete the ballot online, click on the circles next to your candidates to select them. You can also type in candidates where indicated.



# 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

P69-SMD-11-ANC-5A.pdf - Adobe Acrobat Pro

File Edit View Document Comments Forms Tools Advanced Window Help

Text Edits Show

1 / 1 Find 100%

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

Save As

Save in: My Documents

No items match your search.

Recent Places

- Desktop
- Libraries
- Computer
- Network

File name: P69-SMD-11-ANC-5A.pdf

Save as type: Adobe PDF Files (\*.pdf)

Save Cancel

Settings...

**MAYOR OF THE DISTRICT OF COLUMBIA**

**MEMBER OF THE COUNCIL WARD FIVE**

**MEMBER OF ADVISORY NEIGHBORHOOD COMMISSION 5A DISTRICT ELEVEN**



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

3 Complete Ballot

4 Send Ballot

#### Key Dates

October 1  
Vote-by-Mail service begins

October 22

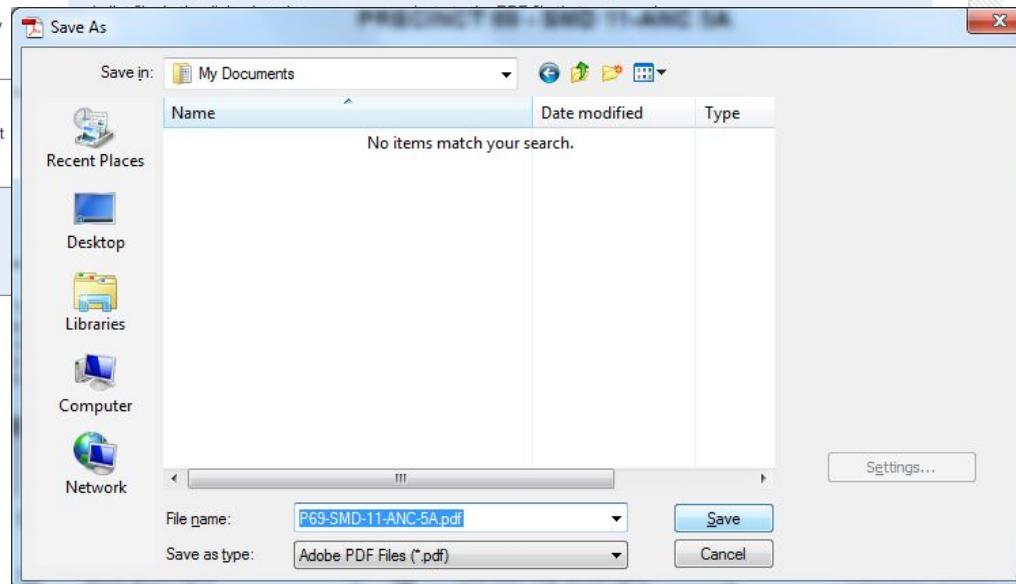
Last day to apply for a  
Vote-by-Mail Ballot

November 2

# Send

#### Locate Ballot PDF and Send

On the web page that is open, select the Choose File button to browse for your





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**

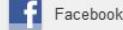
Last day to apply for a  
Vote-by-Mail Ballot

**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

# Recruit



## README.md

# DC Digital VBM

## Requirements

- Ruby 1.8+ (tested on Ruby 1.8.7)
- RubyGems 1.3.6+ (tested on RubyGems 1.3.6)
- Bundler 0.9.26
- GnuPG ([gnupg.org](http://gnupg.org)) with the public key for ballots signing

## Installation (locally)

Get the Bundler:

```
$ sudo gem install bundler --version=0.9.26
```

Get the sources:

```
$ git clone git://github.com/trustthevote/DCdigitalVBM.git
```

Install gem requirements:

```
$ cd DCdigitalVBM  
$ bundle install
```

```
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)}" + @recipient)
      rescue PaperclipCommandLineError
        raise PaperclipError, "couldn't be encrypted. Please try again later."
      end
    end
  end
end
```

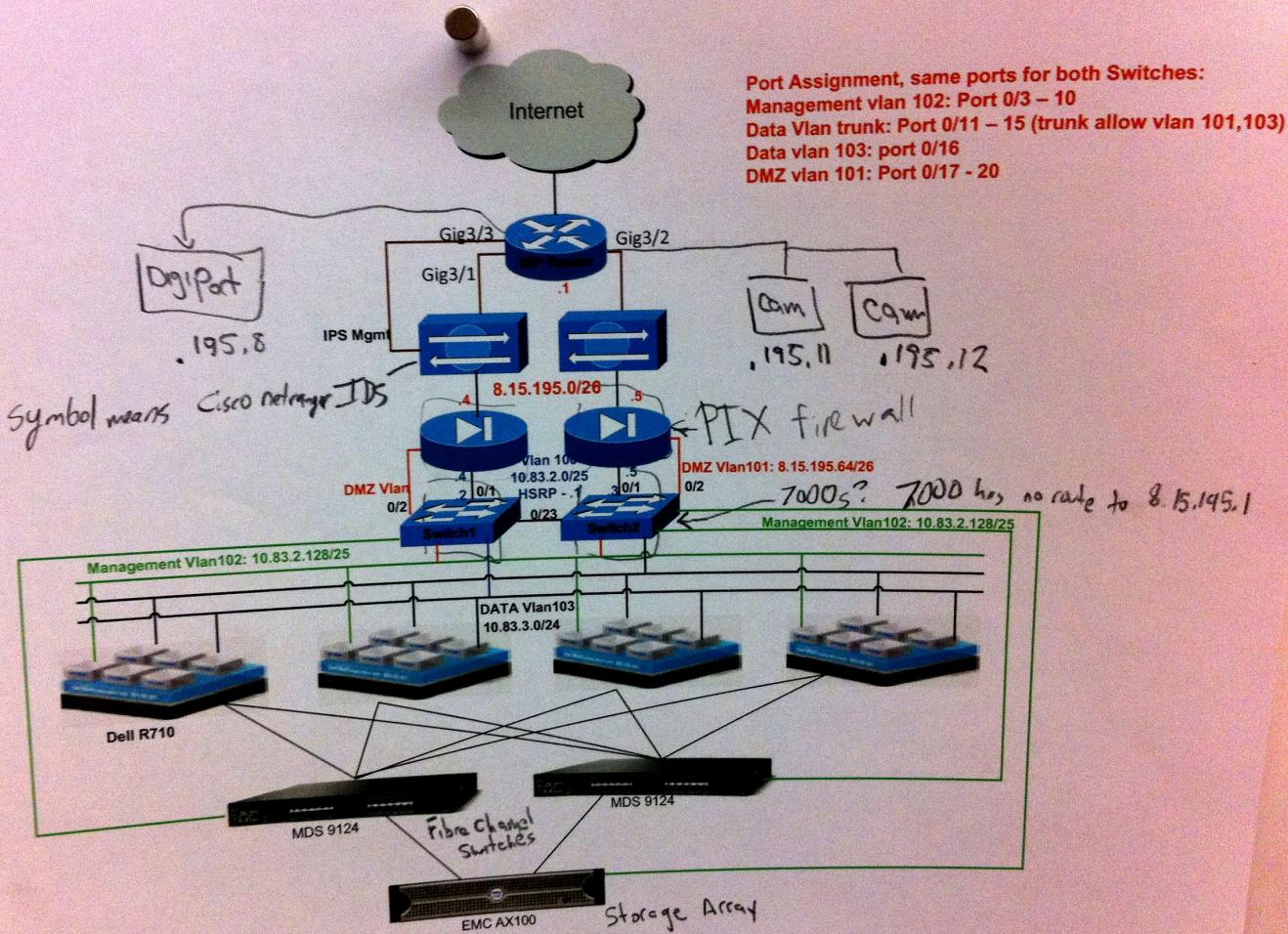
ballot.pdf → /tmp/49d5.pdf

ballot.xyz → /tmp/49d5.xyz

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

# Surveil

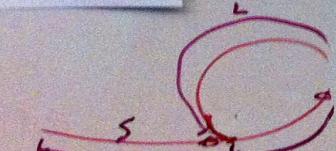
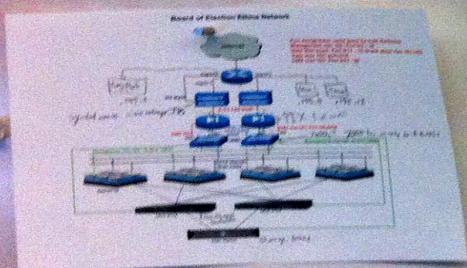
## Board of Election Ethics Network



Mano!  
Port is off  
Alms

Georgia

A. Contactors  
S: SW  
E: HW?  
A: Work w/lan  
E: Look into Infast.



1. Find collision - in loop
2. find size of loop ( $L$ )
3. find collision:  $N - L = S$

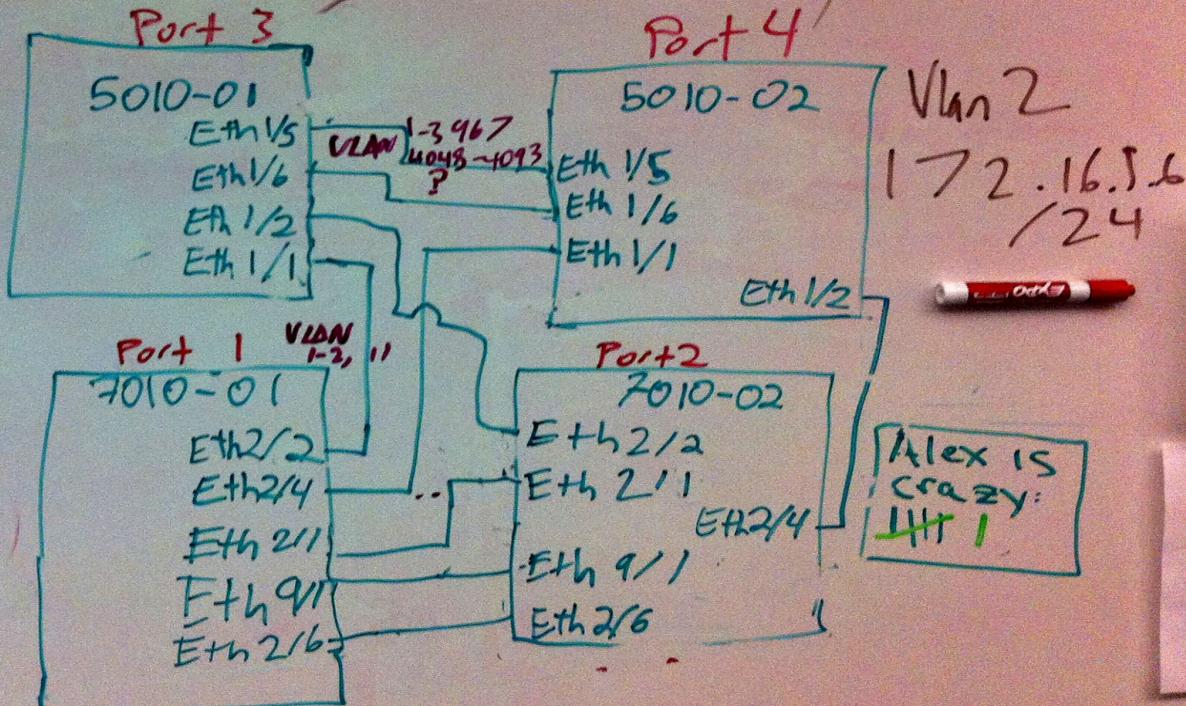
## Switch TODO

1. get Port ↔ computer map (arp?) main?
2. find VPN
3. Tunnel

main?

172.16.1.4

172.16.1.5



Digi Configuration and Management - Mozilla Firefox

File Edit View History Bookmarks Tools Help

8.15.195.8 https://8.15.195.8/useradmin.asp?CURRENT\_PATH=/admin/user\_admin&conf\_root:☆ i Google

Digi Configuration and Mana... +

Additional plugins are required to display all the media on this page.

Install Missing Plugins... x

**Digi Passport™ 8 Configuration and Management**

User : root

**Network**  
**Serial port**  
**Clustering**  
**Power controller**  
**Peripherals**  
**Custom menu**  
**System status & log**  
**System administration**  
**User administration** (selected)  
Access lists  
Change password  
Device name  
Date and time  
Configuration management  
Security profile  
Firmware upgrade  
CLI configuration

**System statistics**

Activate Passport Locator LED  
Apply Changes  
Login as a different user  
Logout  
Reboot

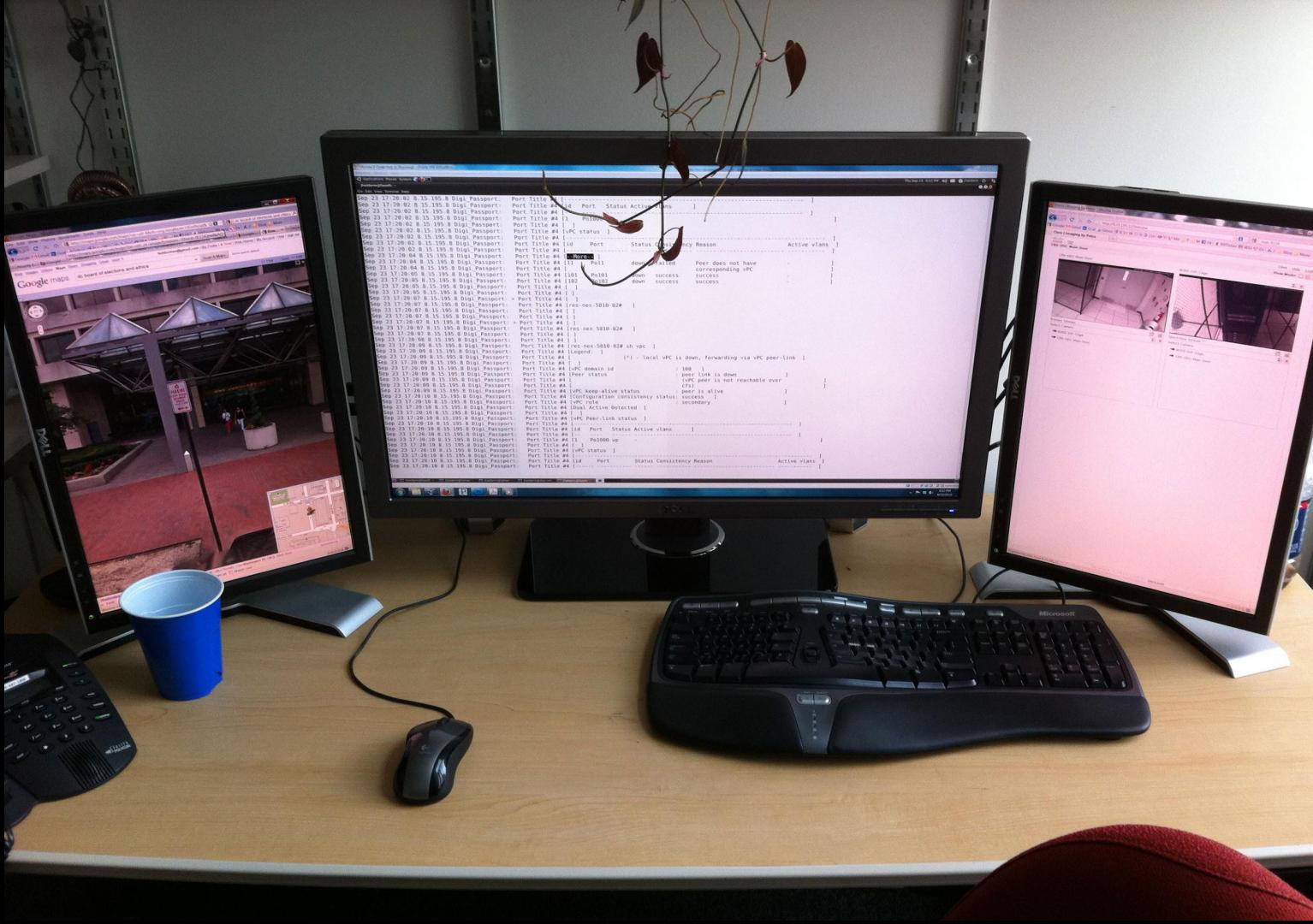
**User administration**  
/ admin / user\_admin

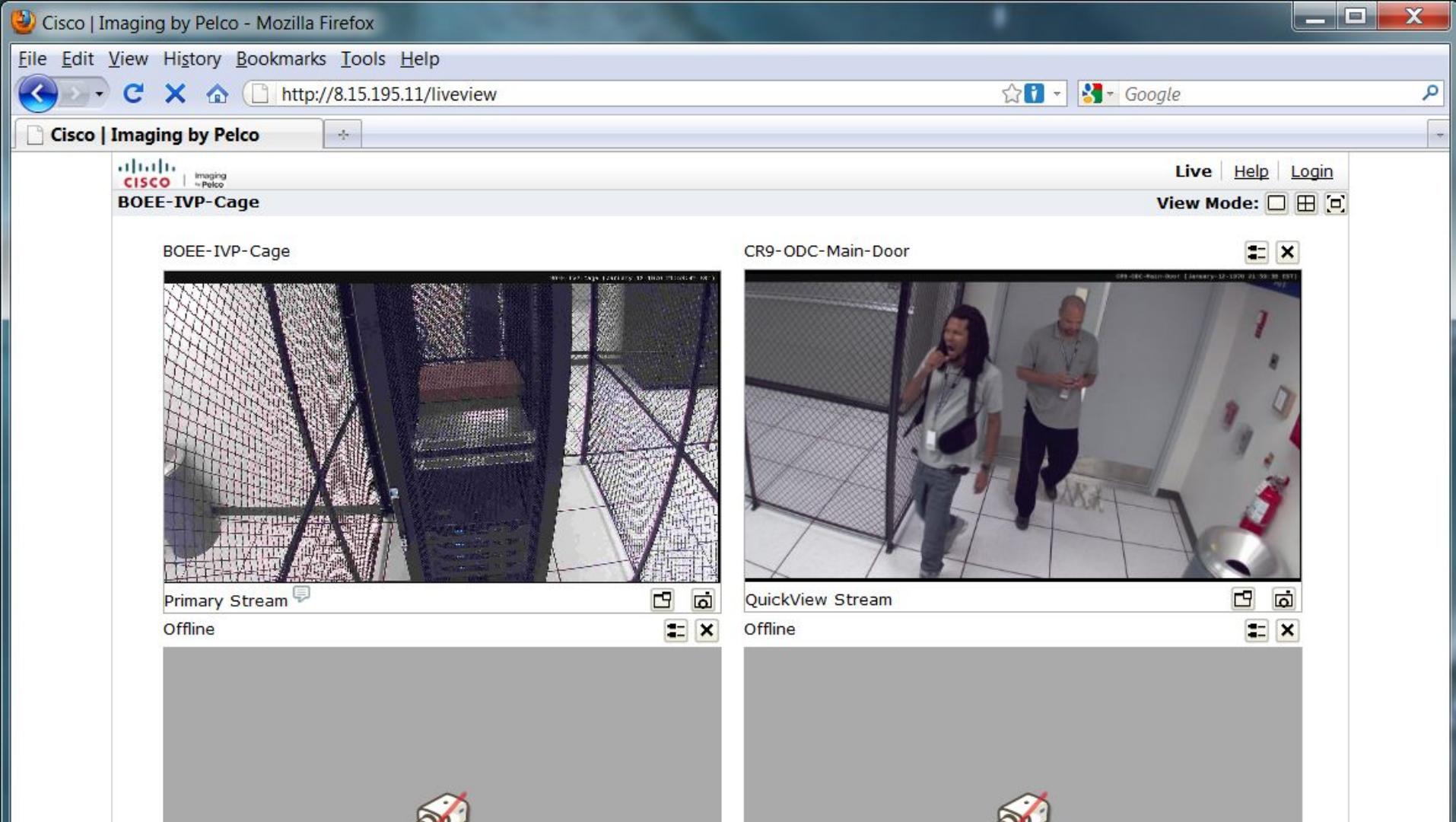
User name :  User group : All group  Locked

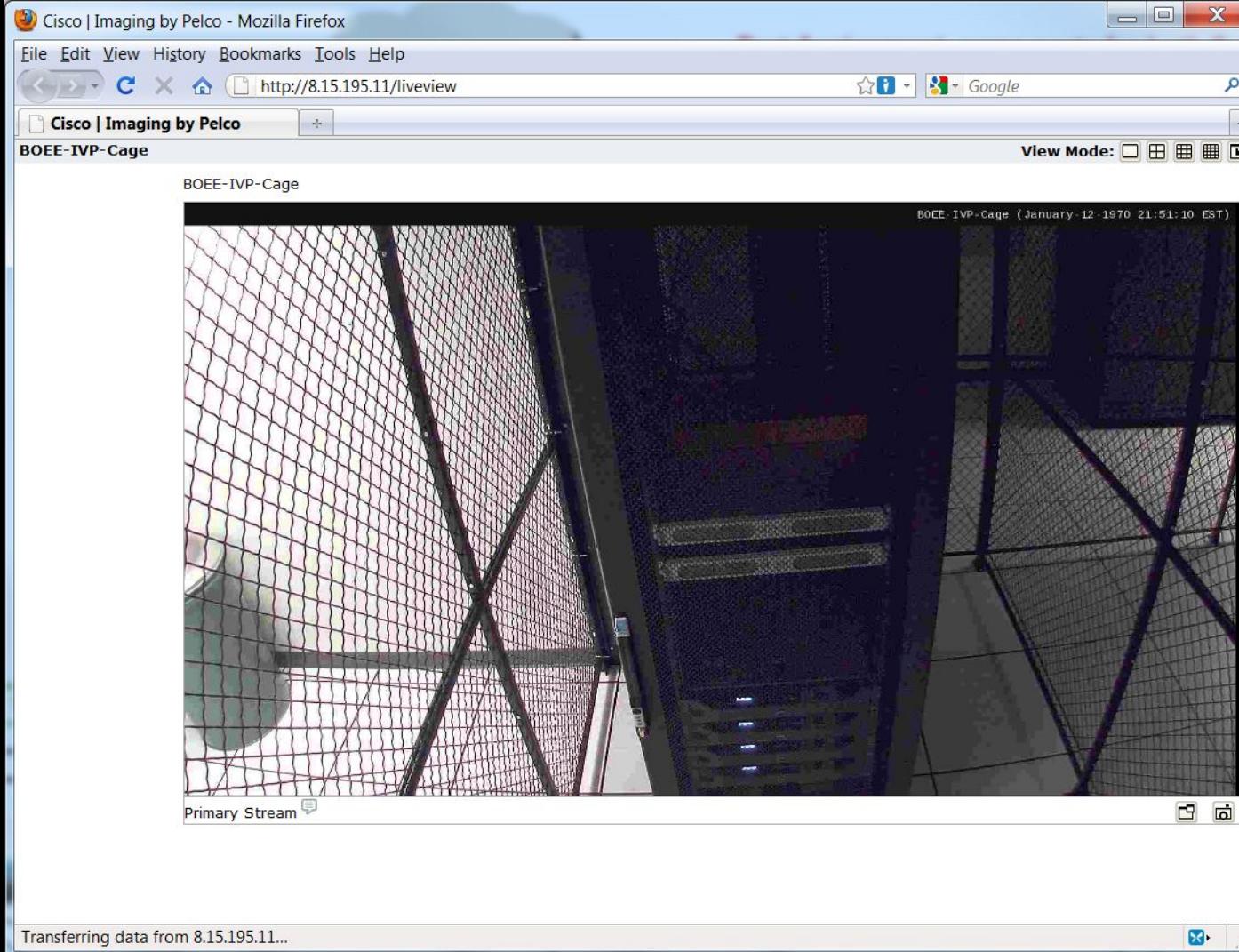
**Current local users**

#	User name	User group	Shell
1	Hoang	System admin	Configuration menu
2	admin	System admin	Configuration menu
3	lle	System admin	Configuration menu
4	oceee	System admin	Configuration menu
5	root	Root	CLI

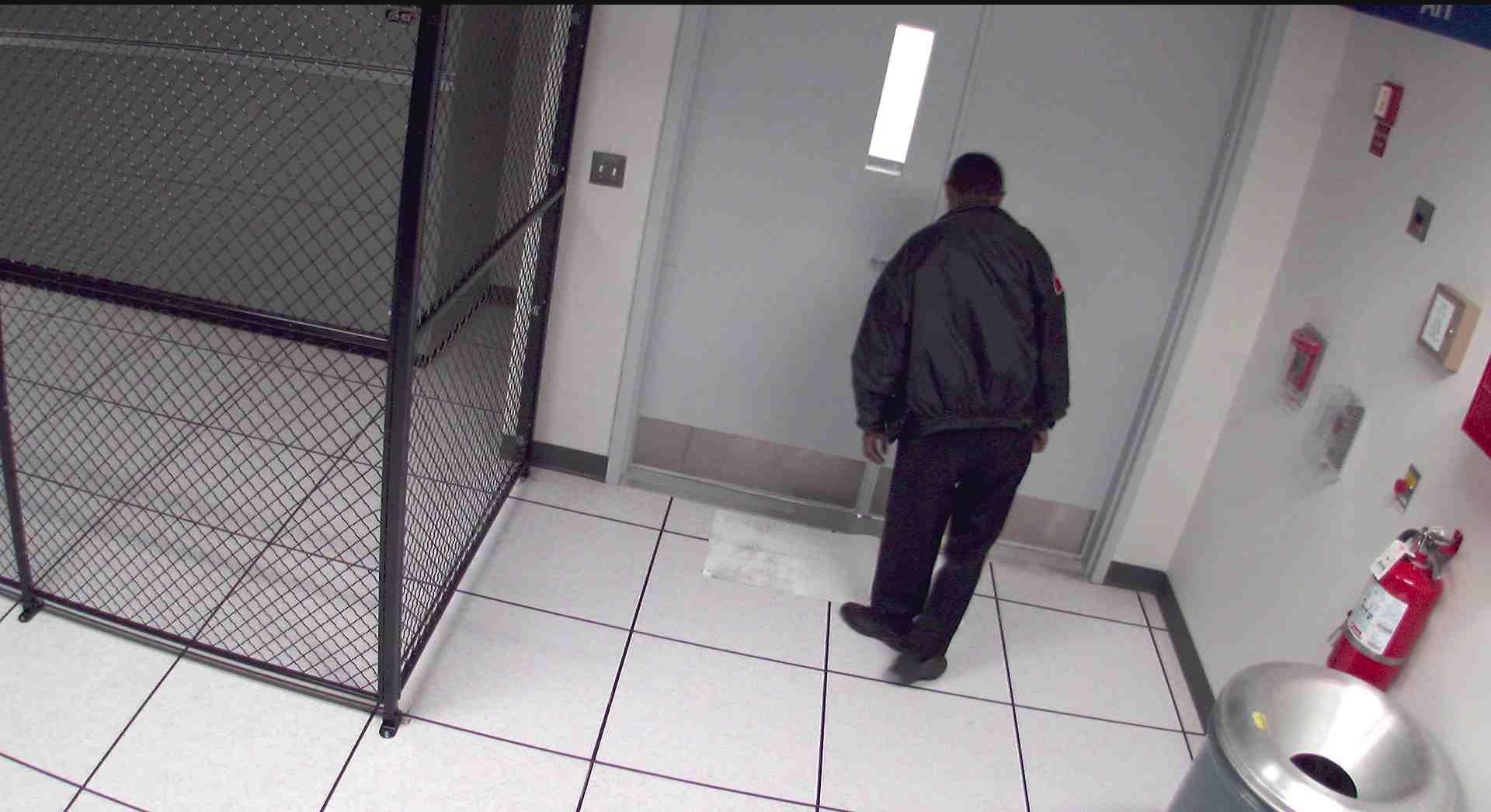
Copyright © 1996-2007 Digi International. All rights reserved.



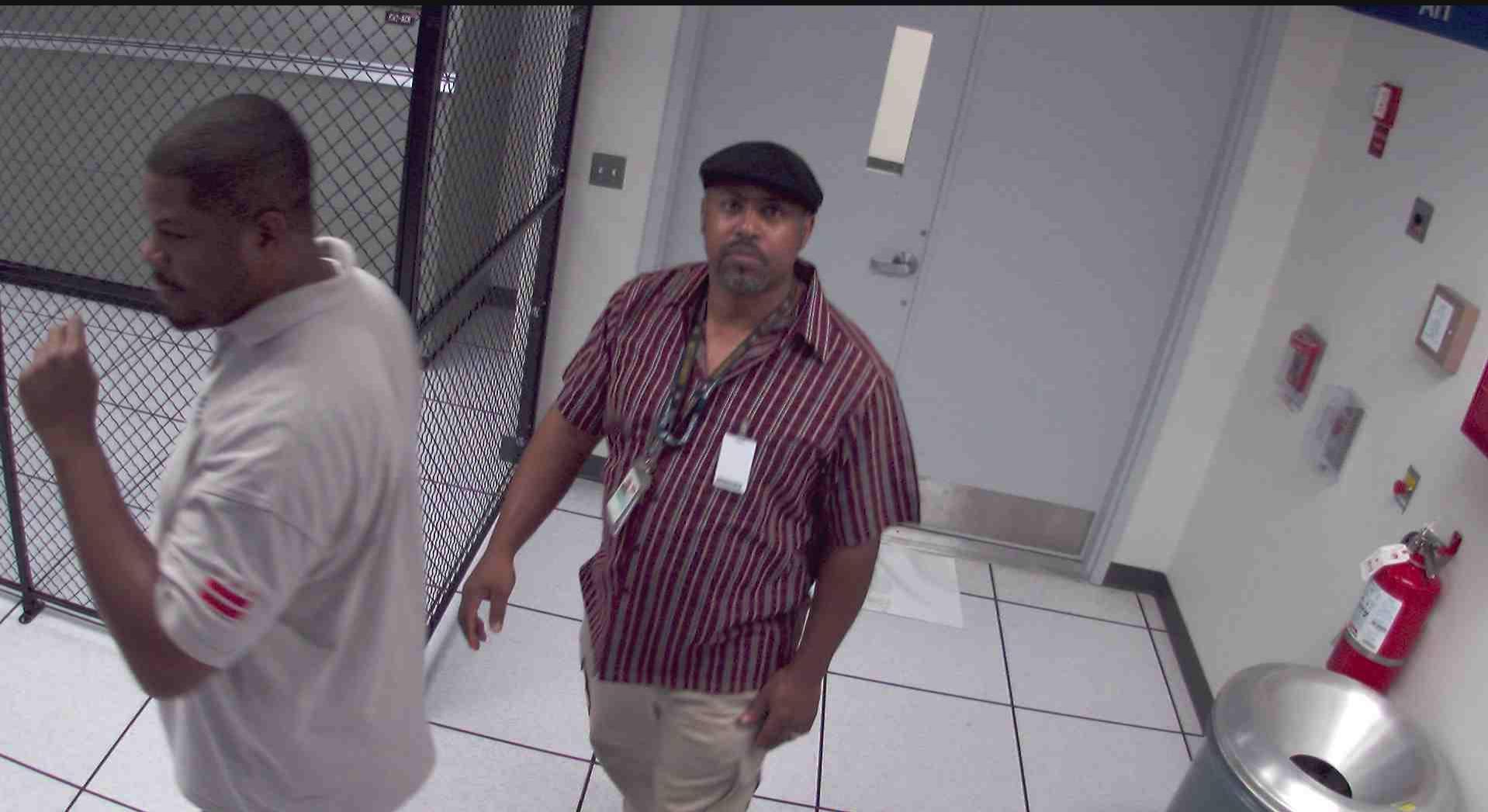
















**Attack!** Steal database credentials, keys, logs, etc.  
Replace all existing votes with our choices

**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 credentials, keys, logs, etc.
- Replace all existing votes with our choices
- Replace any new votes
- Back door to reveal new votes
- Clear logs
- “Calling card”

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

# What about blockchain?

**Blockchain solves stolen votes about as well as Bitcoin solves stolen money.**

Safely voting online requires solving **three major challenges**:

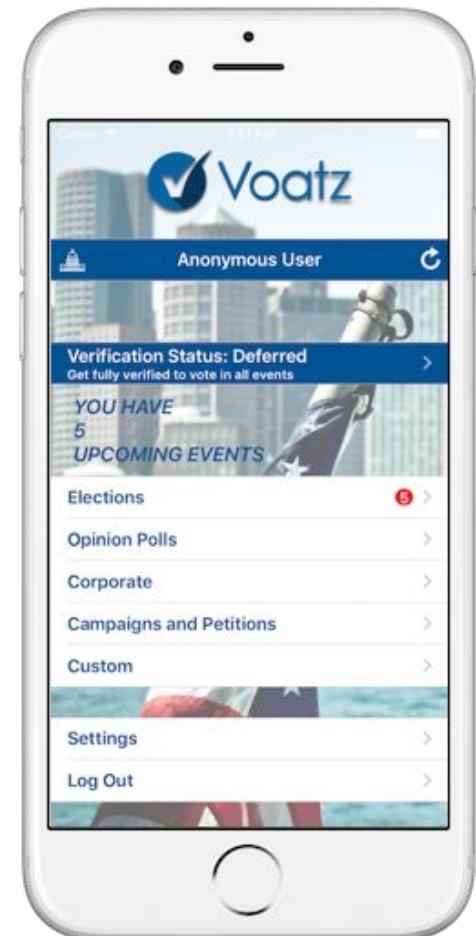
- Casting securely from untrusted user devices.
- Defending servers against nation-state attackers.
- Remotely authenticating voters.

**Blockchain solves none of these.**

Blockchain-based Internet voting piloted by West Virginia in 2018 for overseas voters

- MIT researchers found major problems
- Client doesn't actually use blockchain!
- Snake oil?

“The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz” Specter, Koppel, and Weitzner (USENIX Security 2020)



# Internet Voting Takeaways

Securing online elections requires solving some of the  
**most challenging open problems** in computer security.

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

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

Research shows promise, but my take:  
**A decade or more** until Internet voting can be adequately  
secured, and not without major security advances.

# End-to-End Verifiable Voting

# End-to-End Verifiability (E2E-V)

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 Verifiability (E2E-V)

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.
- No voter can demonstrate how he or she voted to a third party.



# A Verifiable Receipt



How can the voter verify it's really an encryption of their vote?



Alice Johnson, 123 Main . . .



Bob Ramirez, 79 Oak . . . . .



Carol Wilson, 821 Market . .



# Checking the Result

Alice Johnson, 123 Main ...



Bob Ramirez, 79 Oak .....



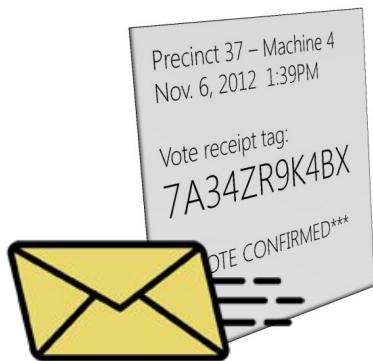
Carol Wilson, 821 Market ...



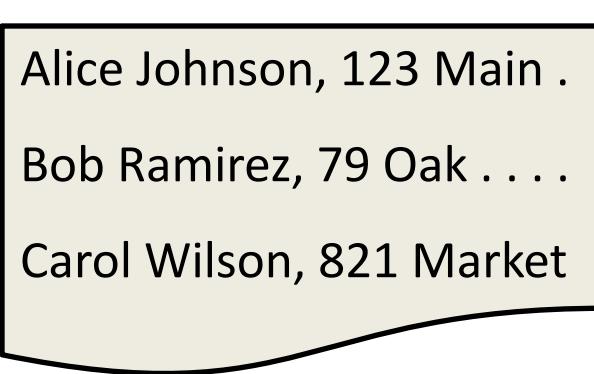
Mathematical  
Proof

# End-to-End Verifiable Elections

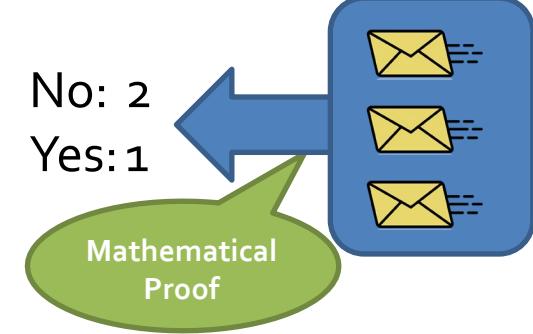
Anyone who cares to do so can:



Check that their own encrypted votes are correctly listed.

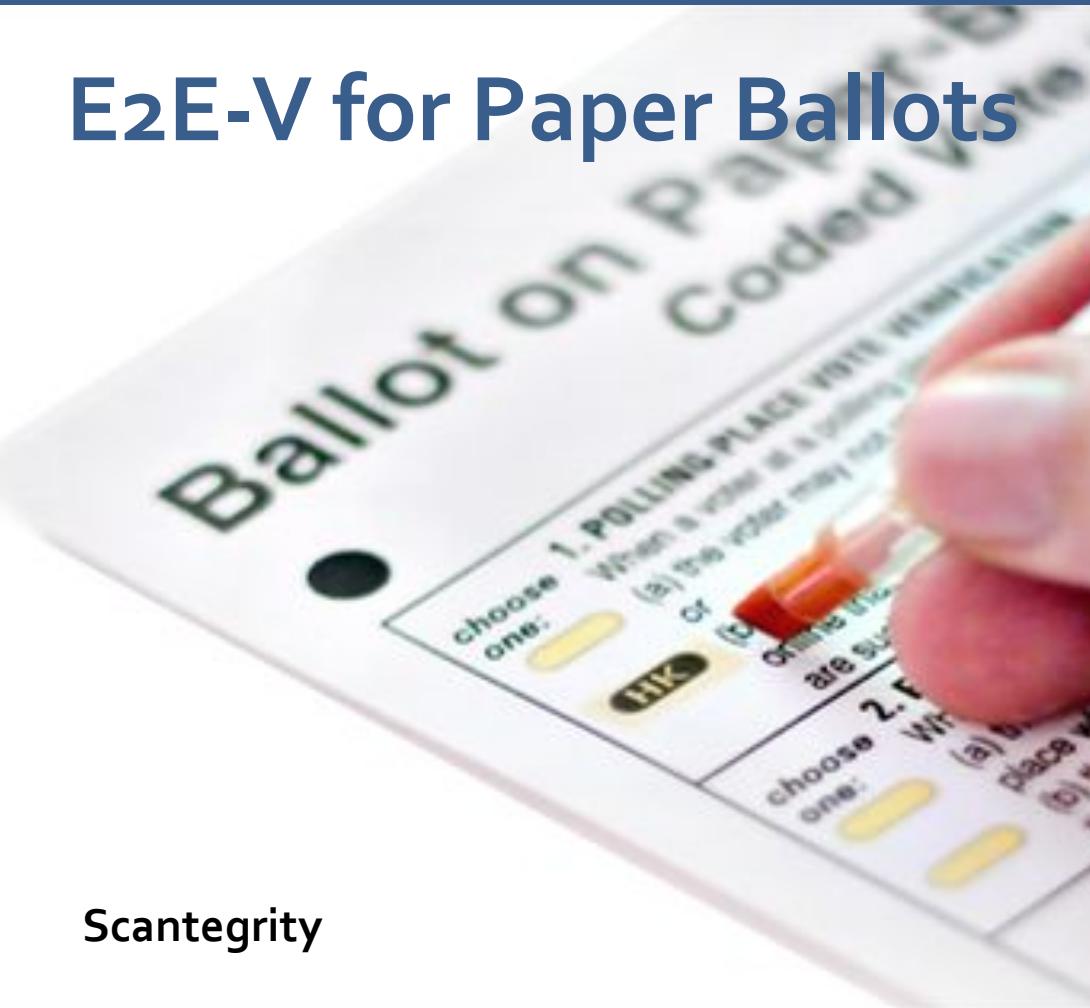


Check that other voters are legitimate.



Check the mathematical proof of the correctness of the tally.

# E2E-V for Paper Ballots



Scantegrity





# Questions for E2E?

Complexity?

Usability?

Comprehensibility?

Security?



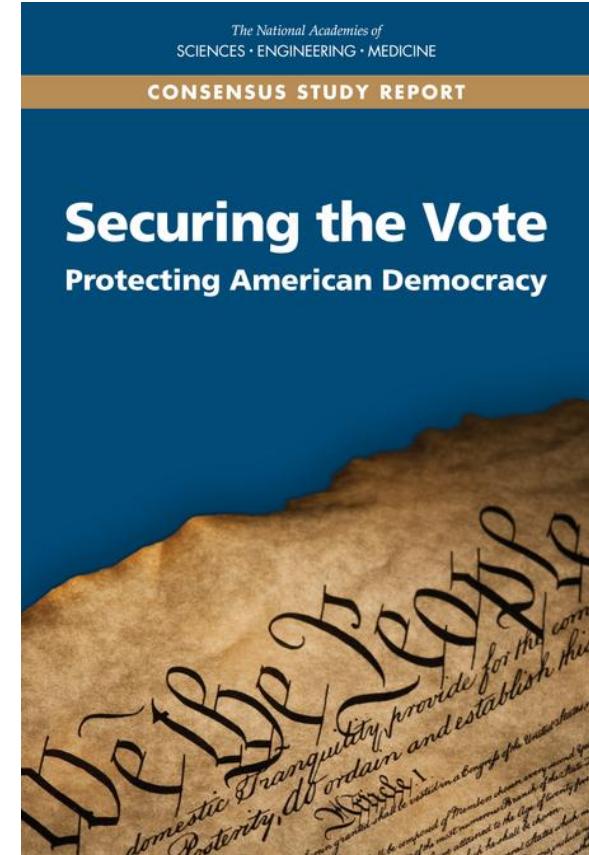
# Defending U.S. Elections

# Key Defenses

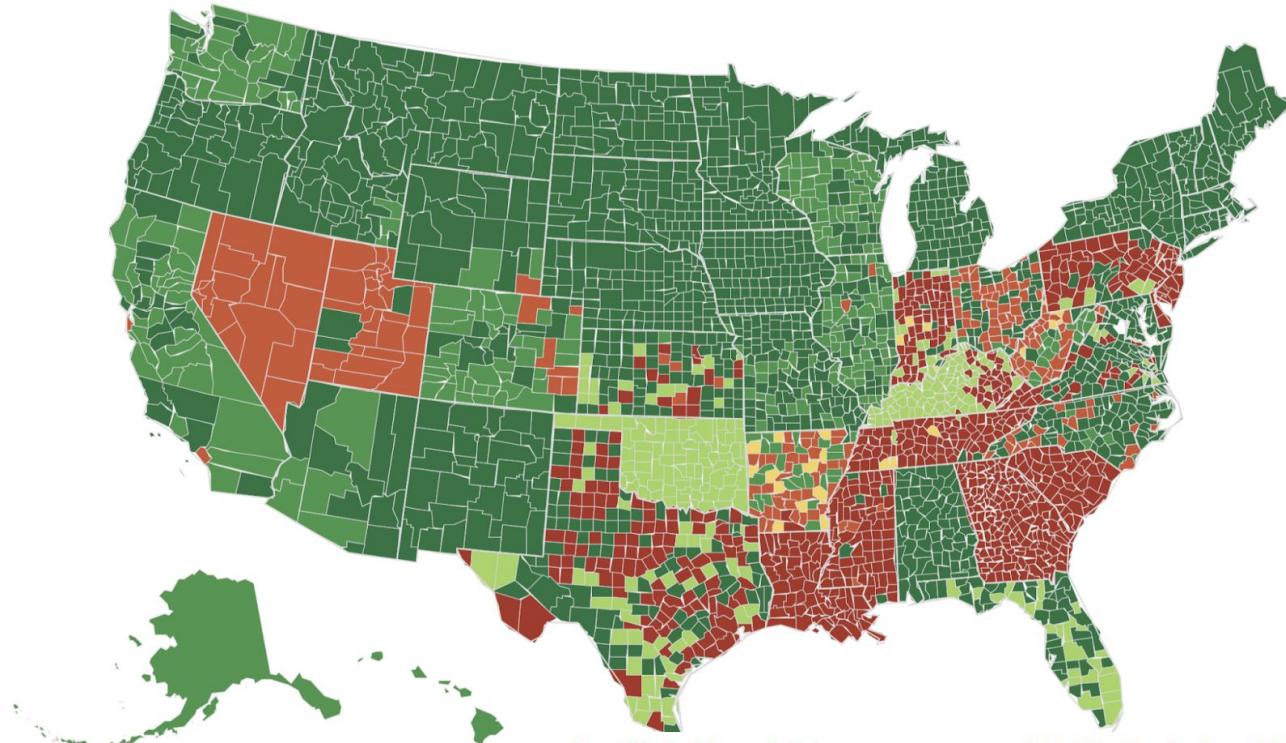
**Consensus** of security experts  
and election officials:

**Paper Ballots + Post-Election Audits**

are a pragmatic, robust, and  
necessary defense.



# Election Equipment in 2016



**70.4%**

Percentage of registered voters living in jurisdictions using Hand Marked Paper Ballots for most voters



**0.7%**

Percentage of registered voters living in jurisdictions using Ballot Marking Devices for all voters

## Direct Recording Electronic (DRE) Systems



**28.9%**

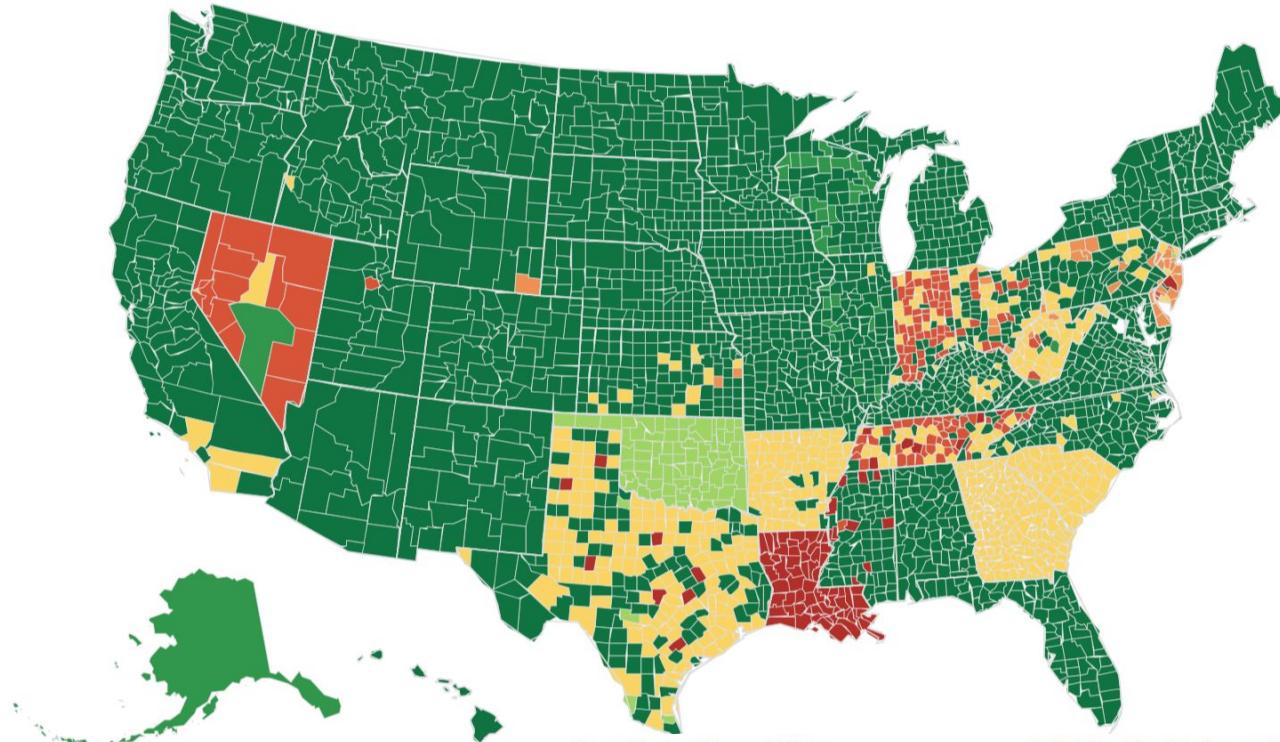
Percentage of registered voters living in jurisdictions using Direct Recording Electronic (DRE) Systems for all voters

## Polling Place Equipment November 2016

- Hand marked paper ballots, with BMDs for accessibility
- Hand marked paper ballots, with DREs with VVPAT for accessibility
- Hand marked paper ballots, with DREs without VVPAT for accessibility
- Ballot Marking Devices for all voters
- Hybrid BMD/Tabulator
- DREs with VVPAT for all voters
- DREs without VVPAT for all voters

# Election Equipment Today

just one state fully paperless



Hand Marked Paper Ballots

**69.2%**

Percentage of registered voters living in jurisdictions using Hand Marked Paper Ballots for most voters

Ballot Marking Devices (BMDs)

**25.5%**

Percentage of registered voters living in jurisdictions using Ballot Marking Devices for all voters

Direct Recording Electronic (DRE) Systems

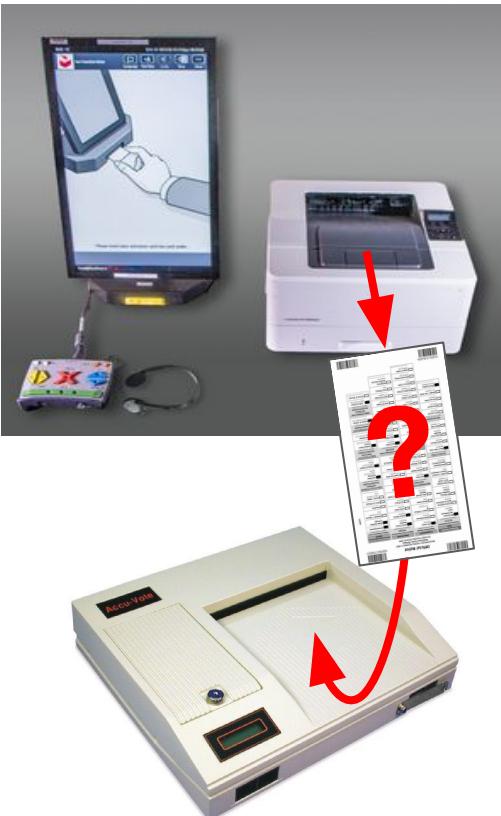
**5.2%**

Percentage of registered voters living in jurisdictions using Direct Recording Electronic (DRE) Systems for all voters

**Verified Voting**

Graphic: <https://verifiedvoting.org/verifier/>

# Universal-Use Ballot Marking Devices



22% of voters live in places that use BMDs for all in-person voting

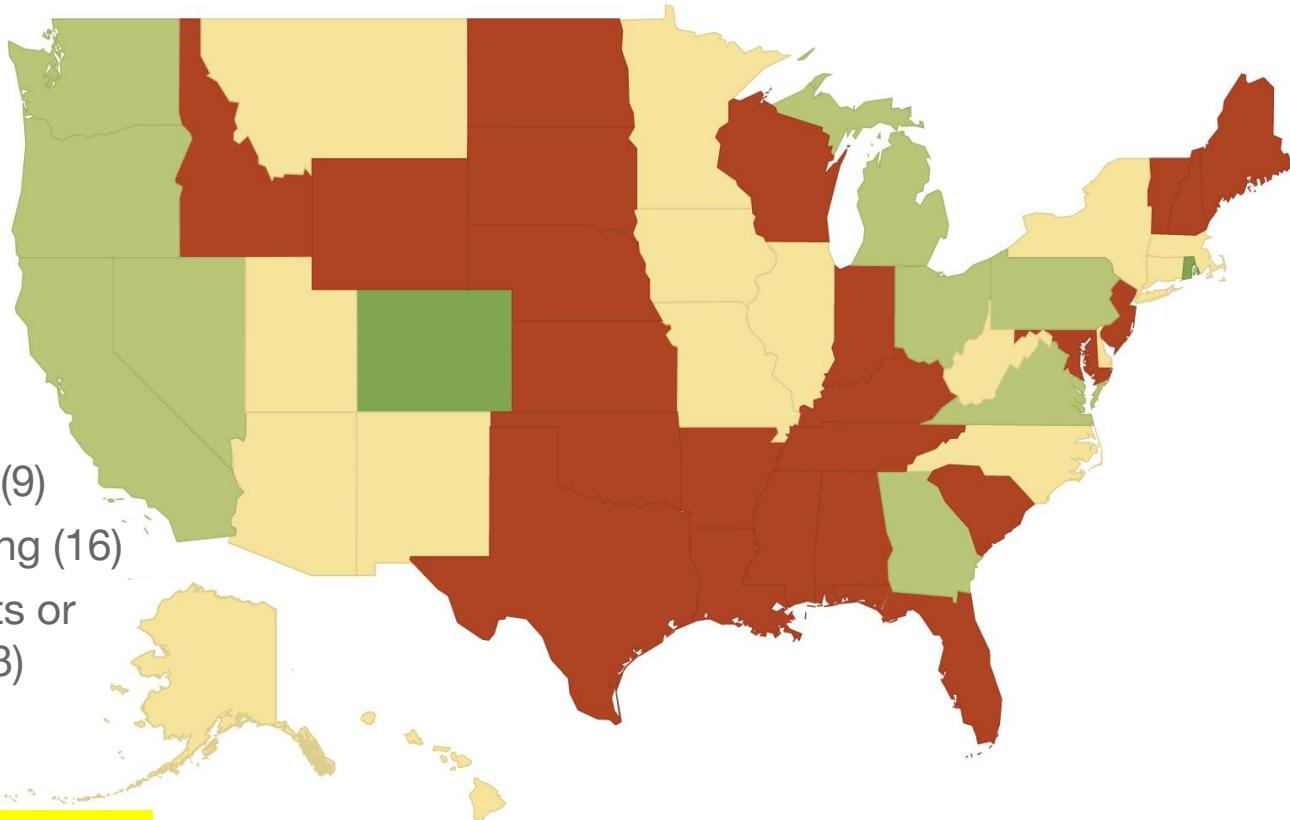
**Threat: Hacked BMDs can change close election outcomes, because many voters don't check the printouts**

In a mock election we conducted, **voters reported <7% of errors.**

- In election with 0.5% margin, hacked BMDs could change outcome while resulting in only 1 problem report per 5000 voters
- **Steps to encourage verification can help, but not enough?**  
If officials investigate when problem reports exceed 1% of voters, need voters to report >80% of errors to spot outcome-changing fraud
- **Using BMDs exclusively for accessibility is much safer**  
If only 1.8% of voters use BMDs, need just 6.7% detection

# States Without Rigorous Audits

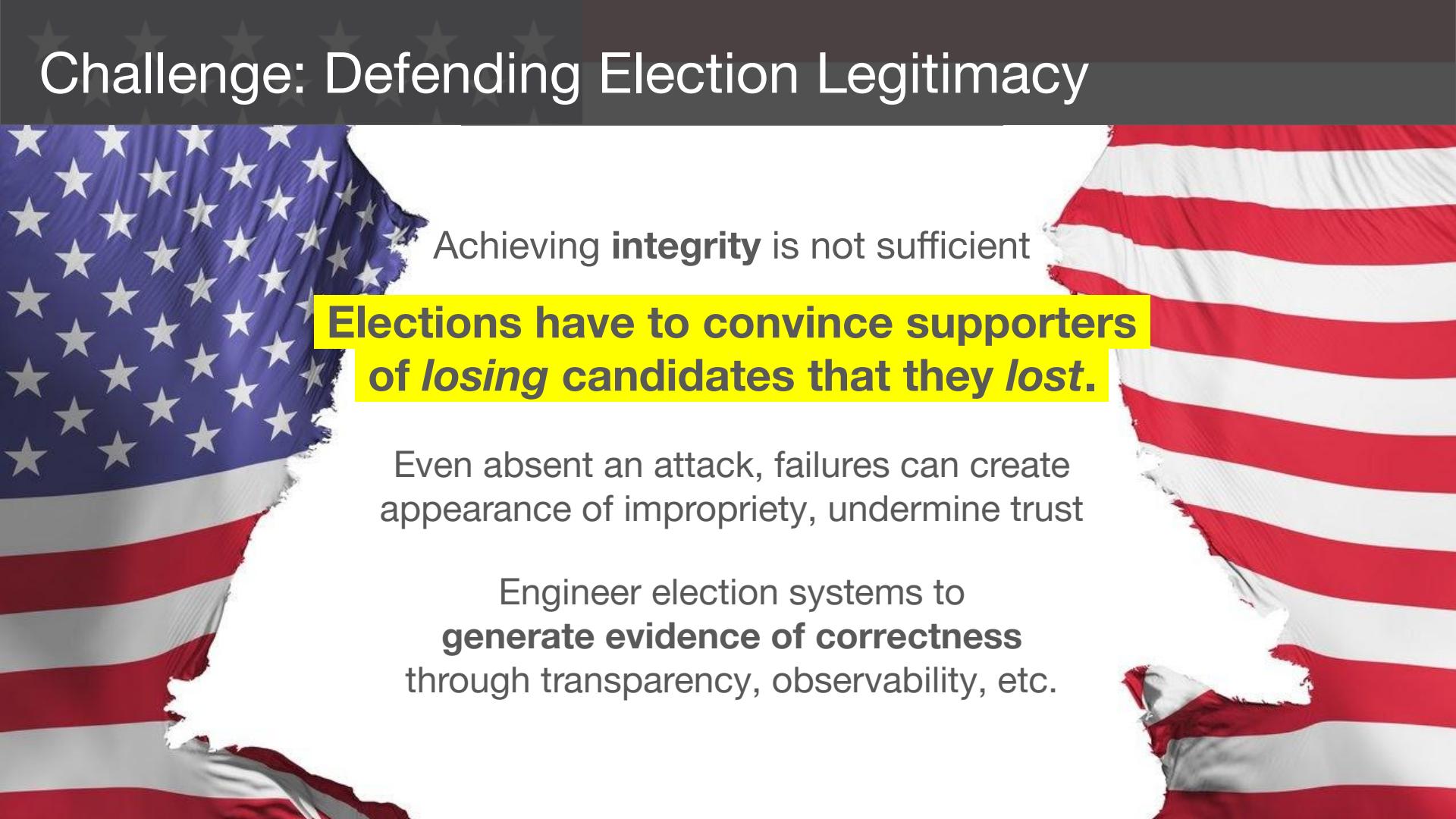
Are votes on  
paper and  
rigorously  
audited?



National cost to audit every  
federal race would be < \$20M/year!

Data: Brennan (2019/08); NCSL (2020/02)

# Challenge: Defending Election Legitimacy

A large American flag is visible in the background, with its stars and stripes partially torn or frayed at the edges, symbolizing damage or conflict.

Achieving **integrity** is not sufficient

**Elections have to convince supporters  
of losing candidates that they *lost*.**

Even absent an attack, failures can create appearance of impropriety, undermine trust

Engineer election systems to  
**generate evidence of correctness**  
through transparency, observability, etc.



Conspiracy theories are an attack on our elections

Only possible because elections *really* are  
much less secure than needed

Skeptical voters deserve a  
reasoned basis for trust

# Progress in Michigan

Paper Ballots?

Yes

Michigan uses paper ballots statewide



Robust Audits?

Progressing

Michigan piloted state-wide RLAs several times since the 2020 presidential election

Requires participation from all local jurisdictions for full implements

So far, these RLAs cover only a single contest

State should routinely conduct RLAs in all major contests

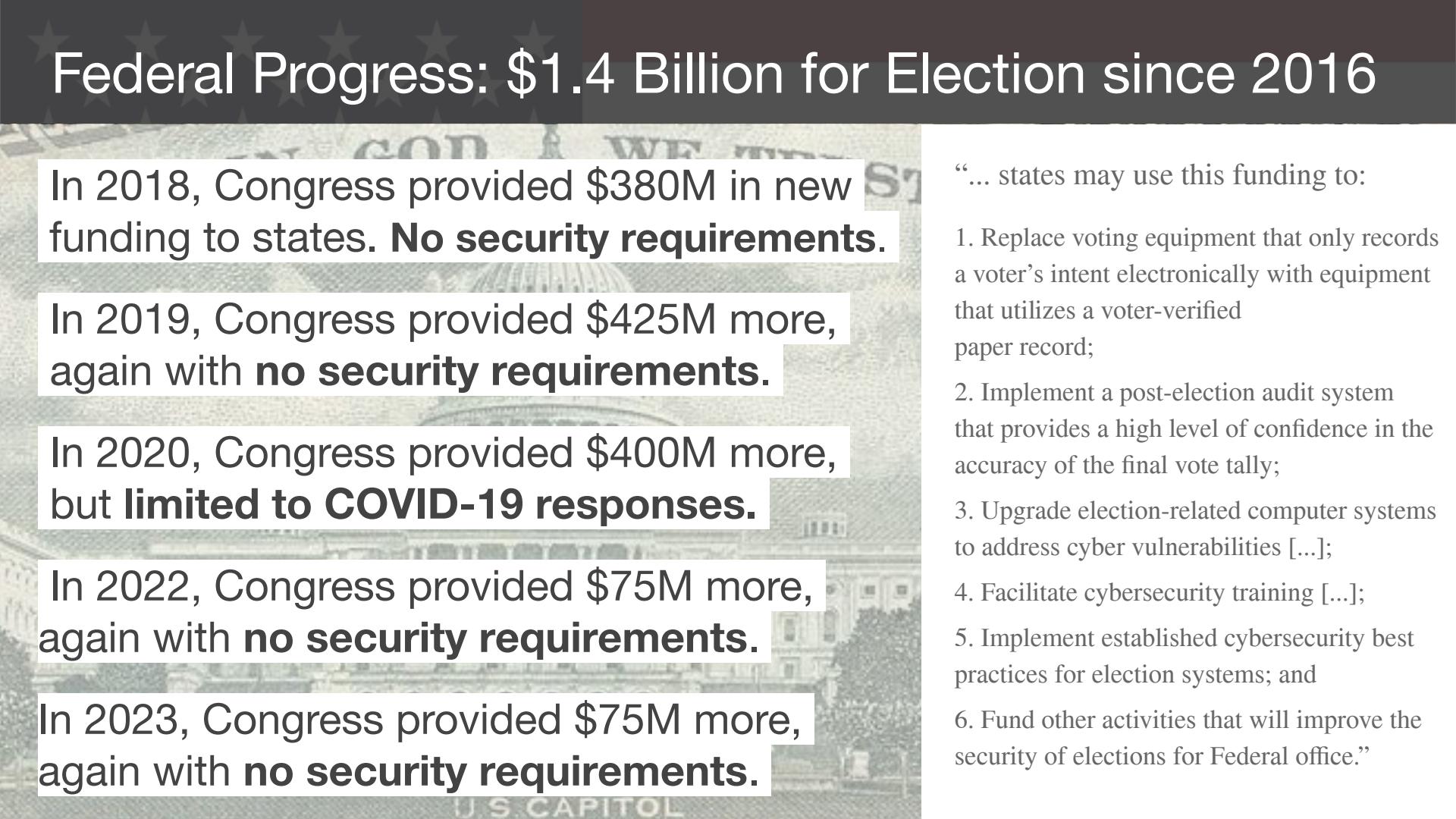


Overall Grade

B+

To get an A,  
Michigan needs  
to finish  
implementing  
RLAs statewide

# Federal Progress: \$1.4 Billion for Election since 2016



In 2018, Congress provided \$380M in new funding to states. **No security requirements.**

In 2019, Congress provided \$425M more, again with **no security requirements.**

In 2020, Congress provided \$400M more, but **limited to COVID-19 responses.**

In 2022, Congress provided \$75M more, again with **no security requirements.**

In 2023, Congress provided \$75M more, again with **no security requirements.**

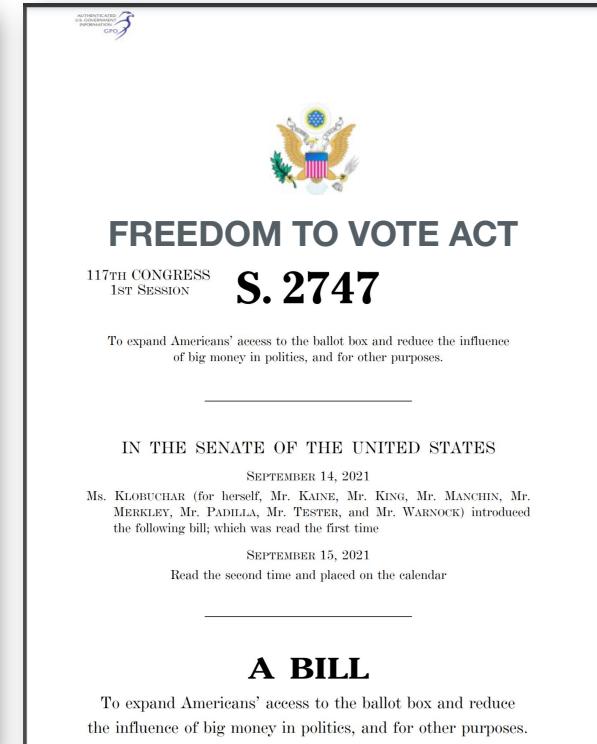
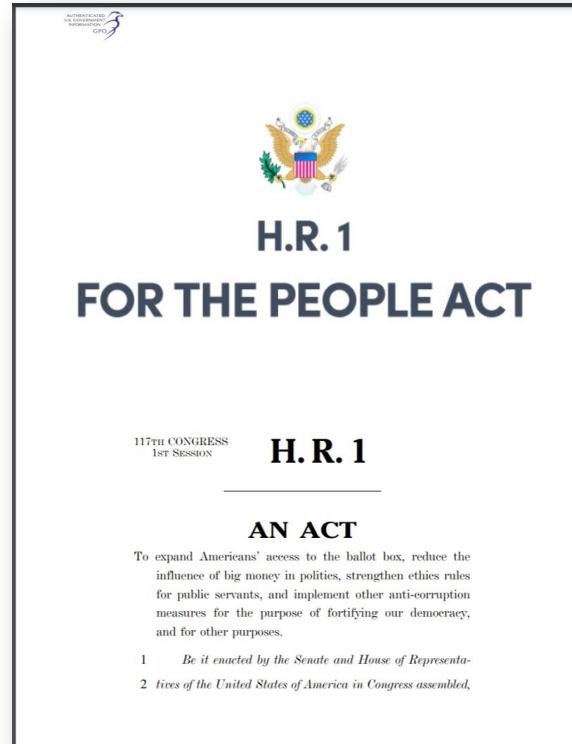
“... states may use this funding to:

1. Replace voting equipment that only records a voter’s intent electronically with equipment that utilizes a voter-verified paper record;
2. Implement a post-election audit system that provides a high level of confidence in the accuracy of the final vote tally;
3. Upgrade election-related computer systems to address cyber vulnerabilities [...];
4. Facilitate cybersecurity training [...];
5. Implement established cybersecurity best practices for election systems; and
6. Fund other activities that will improve the security of elections for Federal office.”

# Congress has an Opportunity to Enact Key Reforms

Election security has been a major component of flagship legislation proposed in the House and Senate

- **Require paper ballots**
- **Risk-limiting audits**
- **Regulate election security vendors**



# Election Security: A complex problem we can solve

No evidence past U.S. election results were hacked ... *what about next time?*

Future elections are vulnerable to *both real attacks and false accusations of fraud*

**Evidence-based methods can show election outcomes are *correct*, not merely that there's “no evidence” they're fraudulent.**

Key reforms:

- Make attacks more difficult: **Apply security testing and best practices**
- Ensure attacks are detectable: **Record every vote on a voter-verified paper ballot**
- Use the paper trail as a defense: **Conduct risk-limiting audits in every election**

# What You Can Do

## As a technologist:

- Accurately explain election security threats and counter disinformation
- Build technology to help make voting on paper easier and more efficient
- Engage with election officials and offer technical expertise

## As a citizen:

- Volunteer as a poll worker. Get involved with local election integrity groups
- Urge officials to implement paper and risk-limiting audits
- Ask states and Congress to pass effective election security legislation
- Learn more! Sign up for **Securing Digital Democracy** on Coursera

**2024 Presidential Election is just one year away. Time to get moving!**

# Coming Up



Reminders:

**AppSec Project due next week, November 16 at 6 p.m.**

Thursday – **Only via Zoom**

**Machine Learning Security**

Guest Lecture by  
**Prof. Kixin Pei**  
(U. Chicago)

Tuesday

**Computer Forensics**

Data collection, forensic analysis,  
anti-forensic techniques