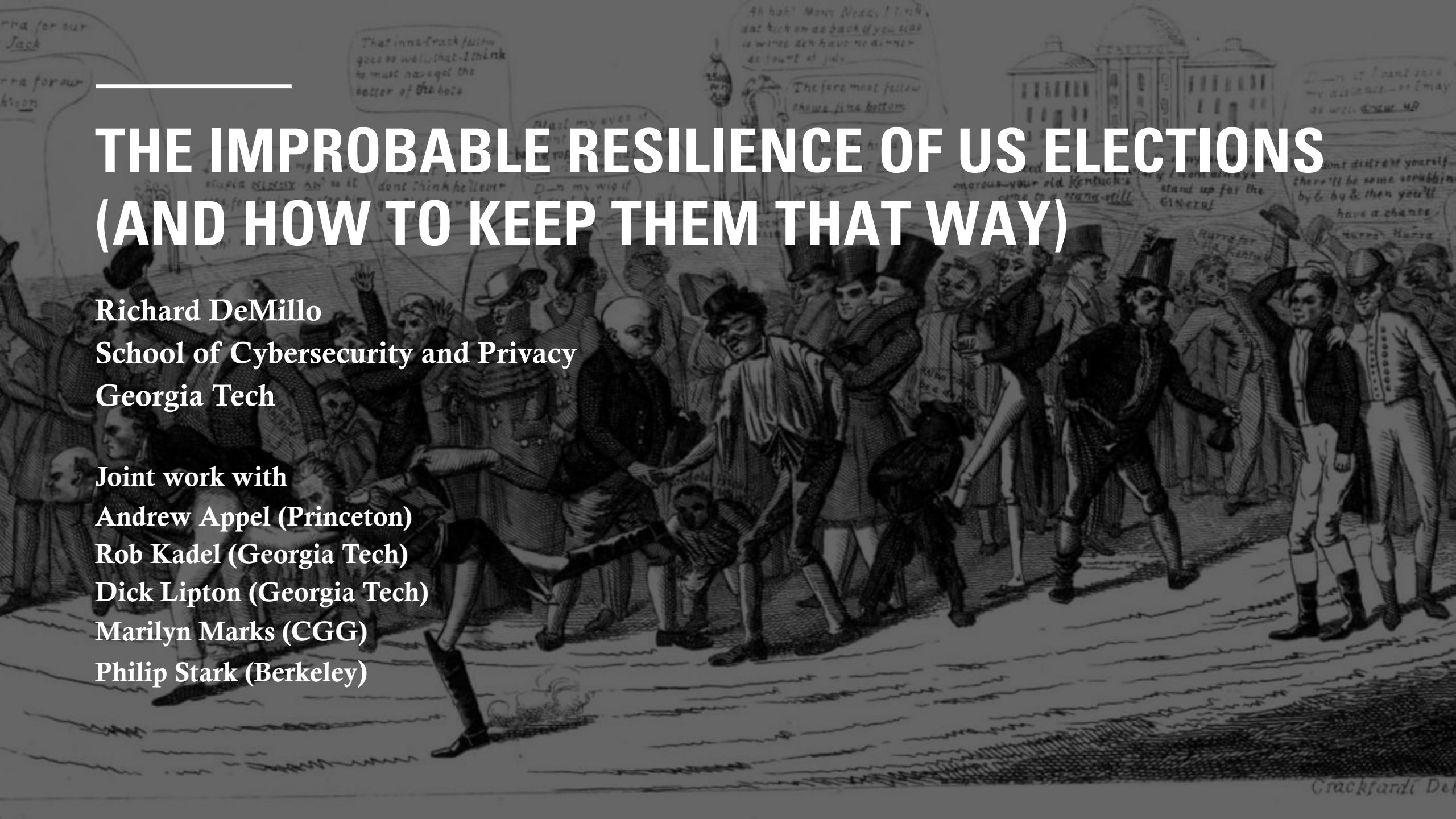
THE IMPROBABLE RESILIENCE OF US ELECTIONS (AND HOW TO KEEP THEM THAT WAY)

Richard DeMillo
School of Cybersecurity and Privacy
Georgia Tech

Joint work with
Andrew Appel (Princeton)
Rob Kadel (Georgia Tech)
Dick Lipton (Georgia Tech)
Marilyn Marks (CGG)
Philip Stark (Berkeley)



Americans' faith in election integrity drops: POLL

Only 20% of the public says it's very confident in the country's elections.

By Brittany Shepherd
January 6, 2022, 6:01 AM

EVERYONE THINKS THIS TIME IS DIFFERENT

RESILIENCE

TRUST

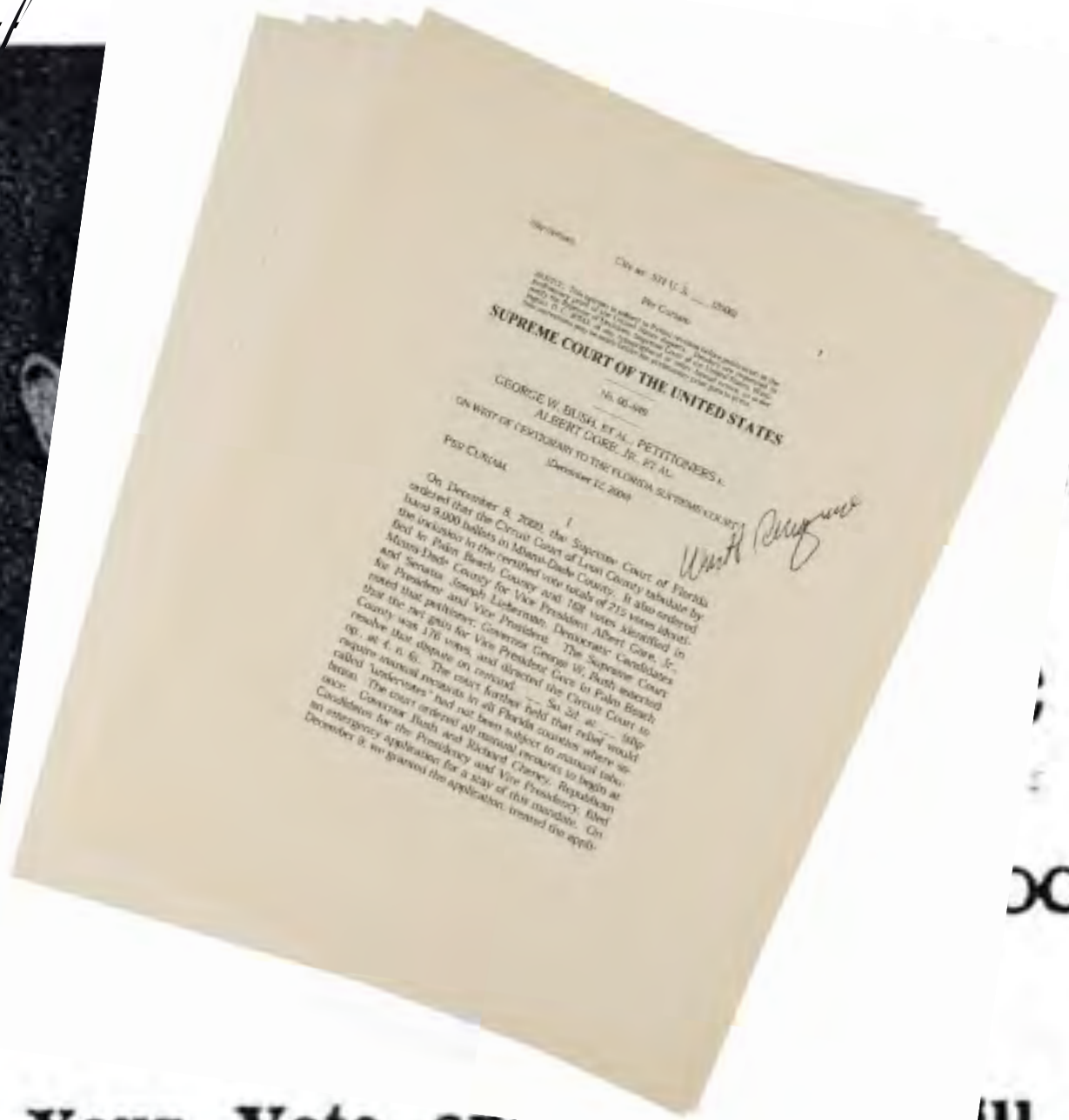
PLAYS NO ROLE IN ELECTIONS

ELECTIONS HAVE TO WORK WHEN PARTICIPANTS MUTUALLY DISTRUSTFUL

U.S. Elections have always been chaotic and prone to corruption

DISTRUST DOES NOT UNDERMINE THE PROCESS

- Donald Trump allies deploy national network of alternate electors to illegally overturn 2020 election results.
- Stolen ballots and coerced votes nearly cost Jimmy Carter his first election in 1962. A county magistrate ruled for Carter.
- Despite probable fraud in Chicago, Richard Nixon did not contest his 1960 loss to John Kennedy
- Samuel Tilden accepted the disputed electoral count of Rutherford Hayes in the compromise of 1877, which ended the Reconstruction
- In "Corrupt Bargain of 1824" House of Representatives made John Quincy Adams President when Henry Clay threw his support to Adams. Andrew Jackson won the popular vote. Clay was named Secretary of State.
- Bush v Gore



SUPREME COURT OF THE UNITED STATES

GEORGE W. BUSH, ET AL., PETITIONERS v.
ALBERT GORE, JR., ET AL.

ON WRIT OF CERTIORARI TO THE FLORIDA SUPREME COURT

PER CURIAM.

Your Vote and

BROOKINGS Election '24 U.S. Economy International

COMMENTARY

How blockchain could improve election transparency

Kevin C. Desouza and Kiran Kabtta Somvanshi
May 30, 2018

The Economist ☰ Men

HARVARD Kennedy School
JOHN F. KENNEDY SCHOOL OF GOVERNMENT

Why American Elections Are Flawed (And How to Fix Them)

Faculty Research Working Paper Series

Pippa Norris
Harvard Kennedy School

September 2016
RWP16-038

United States | Multiple choice

In praise of ranked-choice voting

A simple reform might fix America's dysfunctional politics

BRENNAN CENTER FOR JUSTICE

Search

Issues Our Work Experts Get Involved About Library Press

EXPLORE Our Work

Home / Our Work / Research & Reports / How to Fix American Democracy

Q&A

How to Fix American Democracy

Our government is supposed to be responsive to the will of the people. The For the People Act would mark a major step toward the necessary reforms.



Wendy R. Weiser · Tim Lau

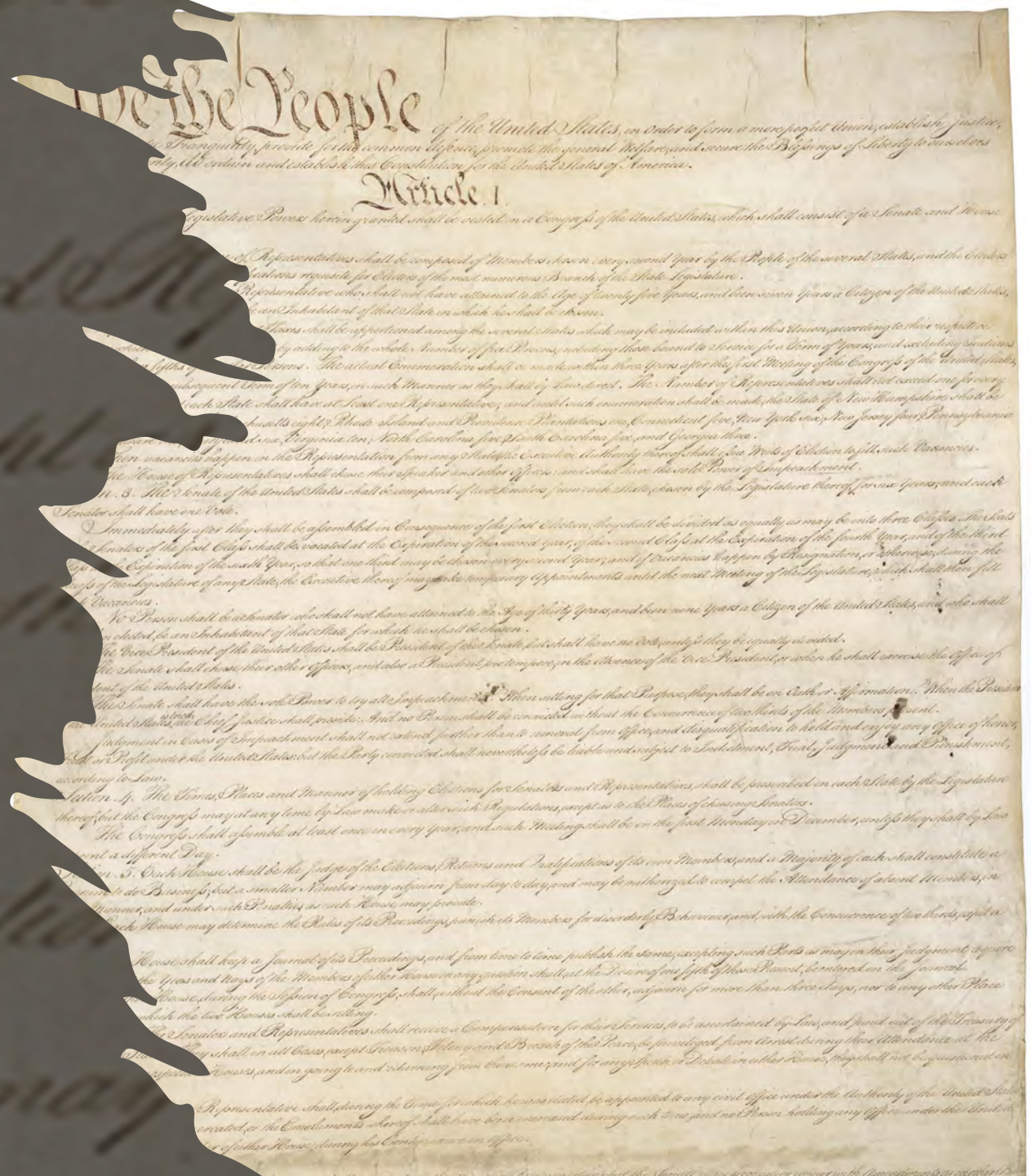
LAST UPDATED: January 20, 2021
PUBLISHED: January 13, 2021

Why doesn't congress step in and fix this mess?

There’s no one in charge

Article 1 Section 4

The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof…



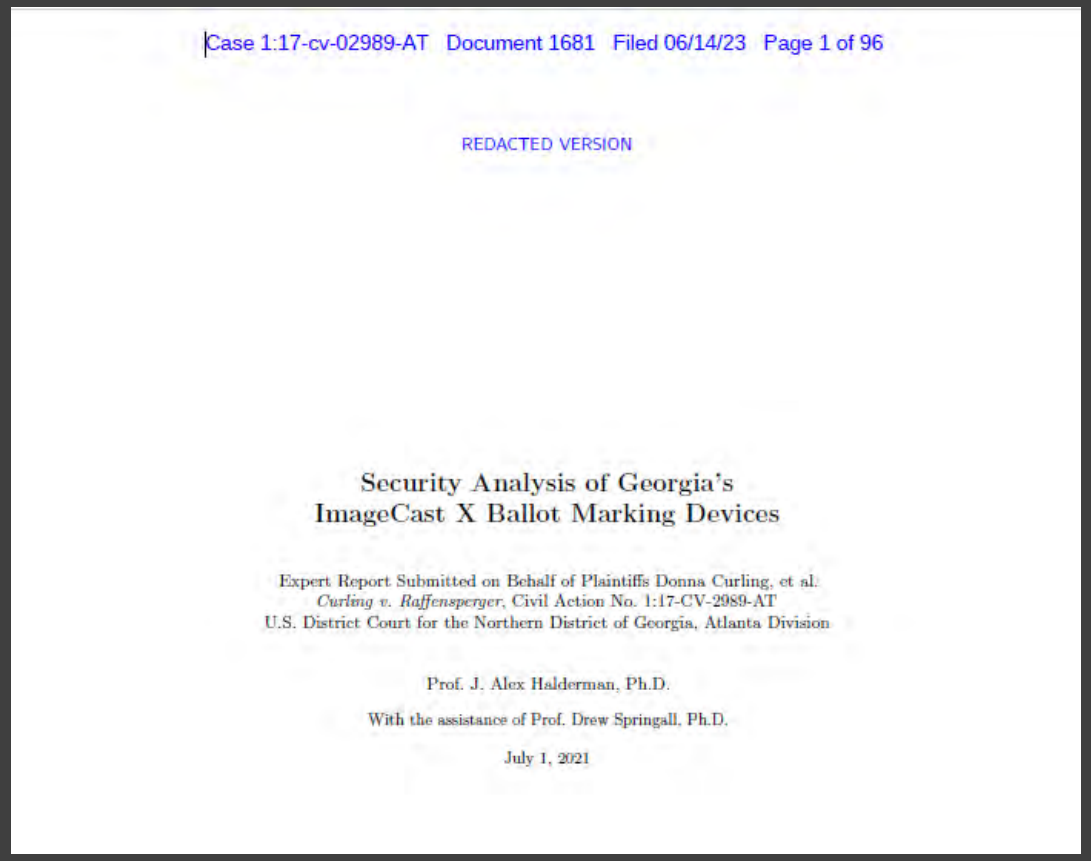
THE 2003 HELP AMERICA VOTE ACT (HAVA) COMPUTERIZED US ELECTIONS

All modern voting machines are computers

2002 Direct Recording Equipment (DRE)

2018 Ballot-Marking Device (BMD)

2020 Vote Centers



Case 1:17-cv-02989-AT Document 1681 Filed 06/14/23 Page 1 of 96

REDACTED VERSION

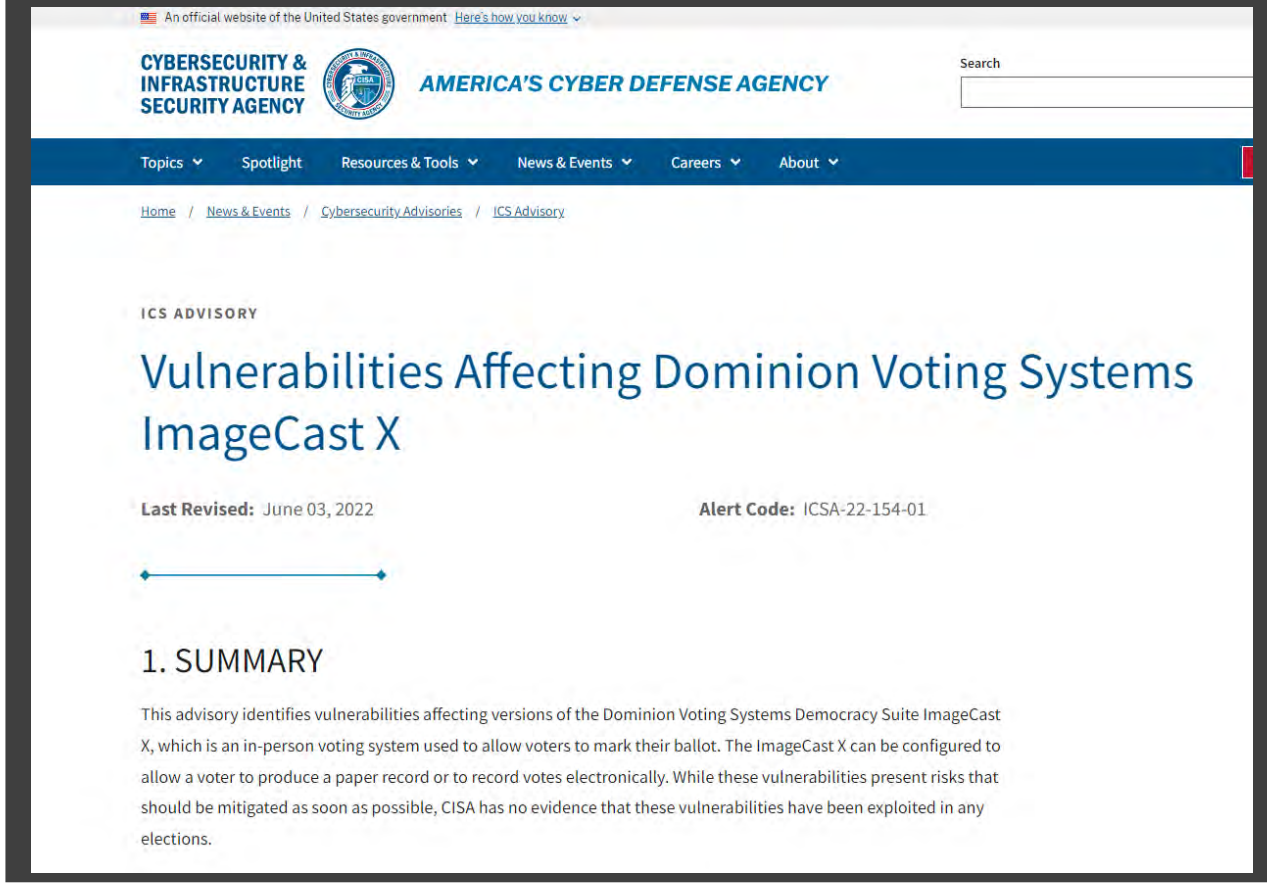
Security Analysis of Georgia's
ImageCast X Ballot Marking Devices

Expert Report Submitted on Behalf of Plaintiffs Donna Curling, et al.
Curling v. Raffensperger, Civil Action No. 1:17-CV-2989-AT
U.S. District Court for the Northern District of Georgia, Atlanta Division

Prof. J. Alex Halderman, Ph.D.

With the assistance of Prof. Drew Springall, Ph.D.

July 1, 2021



An official website of the United States government Here's how you know

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Search

Topics Spotlight Resources & Tools News & Events Careers About

Home / News & Events / Cybersecurity Advisories / ICS Advisory

ICS ADVISORY

Vulnerabilities Affecting Dominion Voting Systems ImageCast X

Last Revised: June 03, 2022

Alert Code: ICSA-22-154-01

1. SUMMARY

This advisory identifies vulnerabilities affecting versions of the Dominion Voting Systems Democracy Suite ImageCast X, which is an in-person voting system used to allow voters to mark their ballot. The ImageCast X can be configured to allow a voter to produce a paper record or to record votes electronically. While these vulnerabilities present risks that should be mitigated as soon as possible, CISA has no evidence that these vulnerabilities have been exploited in any elections.

All computers can be programmed to cheat…
including computers used for voting

“The Court PROHIBITS any use of the GEMS/DRE system after 2019.” Timeline of a constitutional controversy

- 2017: separate §1983* actions against Georgia Election Officials
- Allegation: state’s reliance on DRE voting systems burdened the 14th Amendment rights to due process and equal protection
  - DRE voting machines do not produce a paper trail or any other way to verify each individual’s vote
  - DRE machines have known cybersecurity vulnerabilities
- Other active cases
  - Common Cause v Kemp (insecure voter registration database)
  - Martin v Kemp (voter disenfranchisement)
  - Coalition for Good Governance v Crittenden (undervotes caused by DREs)
- August 2019: Federal Court Judge Amy Totenberg rules DREs unconstitutional**
- January 2024: Trial to rule BMDs unconstitutional***

*Section 1983 of the US Code provides a cause of action for victims of constitutional violations by state or local government officials

**Case 1:17-cv-02989-AT Document 375 Filed 05/21/19

***Case 1:17-cv-02989-AT Document 1705 Filed 11/10/23 (https://freespeechforpeople.org/wp-content/uploads/2023/11/2023-11-10_order_dckt_1705_0.pdf)

Why are we in this pickle?

- Computerized election systems are vulnerable to errors and attacks
- Election officials refuse to acknowledge the likely root causes
- We operate an election infrastructure on 1990’s insecure hardware
- Software vendors with meager resources misrepresent the real security posture of their products
- State officials will not permit the most basic auditing and checking that might detect errors and attacks

Mississippi Plan (1890): “If you keep poor people from voting, you necessarily keep black people from voting”

- Residence requirements
- Poll tax
- Literacy tests
- Cumbersome registration
- Voter disenfranchisement
- Easy-to-conceal corruption
- Safeguarding elections
- Appearance of inclusion
- “Find characteristics you want to exclude” *

*Carol Anderson, *One Person, No Vote*

The 2024 Funnel

Threat

1. Sow distrust
2. Dashboard-enabled ROI
3. Voting rolls
4. Access and scarcity
5. Insiders
6. Bugs and hacks
7. Illusion of fairness
8. Lost votes
9. Incorrect counting
10. Meaningless audits

Enabler

1. Internet-driven amplification
2. Predictive analytics
3. Exact match, purging, security
4. e-pollbooks and voting machines
5. No physical security
6. Opacity
7. Voter verification
8. Complex but meaningless checks
9. Proprietary software
10. Untrusted audit trail

If you want to steer votes, require all voters to use a computer

They’re scarce

You can put them where you want them

Make the logistics unmanageable

Make up security measures that don't exist

The Secretary of State has contracted with ES&S for ballot building support services to "assist" the Center for Election Systems in constructing the GEMS databases that are used within county elections. (*Id.* at 83-84.) Three individuals from ES&S[28] work solely on Georgia election databases and perform "their ballot building work within their own purviews" and construct the GEMS databases on desktop computers from their homes. (*Id.* at 84-85.) According to Barnes, the individuals are subject to the same requirements for using air gapped equipment as the Secretary of State, though he testified he does not know what physical security parameters each of the individuals have within their homes. (*Id.* at 85-

[27] Mr. Barnes often refers to the private computer housing the GEMS server as "air gapped." However, as Dr. Halderman and Dr. Shamos both testified – the actual process used by the Secretary of State's Office does not constitute an "air gapped" system as explained below. The Court will therefore refer to "private" as not being directly connected to the internet.

[28] Two of these individuals previously worked for Barnes at CES and the third worked for Cobb County. (Tr. Vol. 1, Doc. 570 at 85.) Barnes was not aware of whether these individuals were employees of ES&S or independent contractors.

Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials

The top voting machine company in the country insists that its election systems are never connected to the internet. But researchers found 35 of the systems have been connected to the internet for months and possibly years, including in some swing states.

By Kim Zetter

Aug 8 2019, 10:55am Share Tweet

… because insider threats…

On January 7, 2021 Coffee County, GA Election Director Misty Hampton allowed people employed by election denier Sydney Powell access to Georgia's Election Management System to:

1. Make forensic copies
2. Post executables on open servers
3. Modify election records
4. Modify software

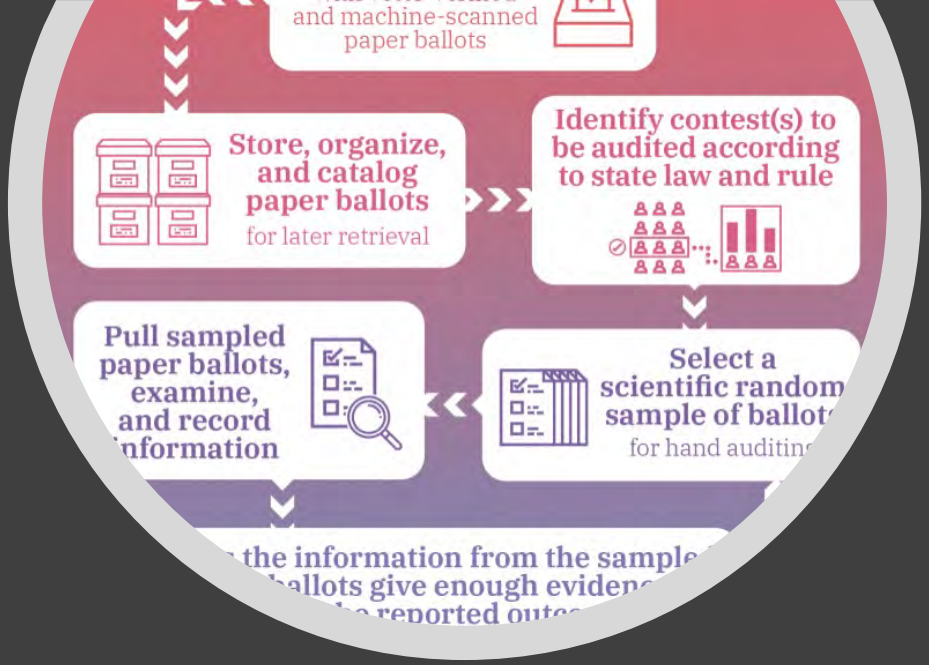
Fail to address the essential security flaw of Ballot-Marking Devices*

There is no way to prevent undetected discrepancies between what voters see on the screen and what is recorded

If voters notice, there is no appropriate remedy

*Appel, DeMillo, Stark, *Ballot-Marking Devices Cannot Assure the Will of the Voter,* **Election Law Journal, Vol. 19(3), 2020**
DOI:10.1089/elj.2019.0619

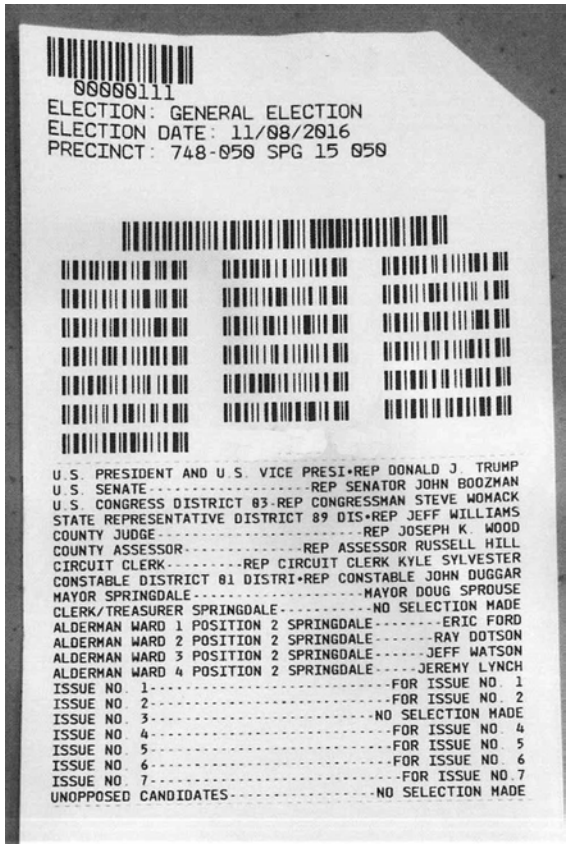
Make Audits Meaningless



RLA's REQUIRE A VERIFIED AUDIT TRAIL

If the ballot pool is polluted, you can't conclude anything about the reported outcome!

Ballot Verification is a literacy test



- ≈50% did not look at the paper ballots at all
- Just looking is a complex cognitive task
  - Barcodes
  - Parsing the card
  - Detecting errors 10x harder than preventing them to begin with
  - 50% error rates for cognitively similar tasks
- Of those who looked:
  - 222ms per contest
  - ≈ 50% unable to correctly identify the ballot they had just voted
- An attacker who changes 10% of the ballots has a 9.95% chance of not being detected

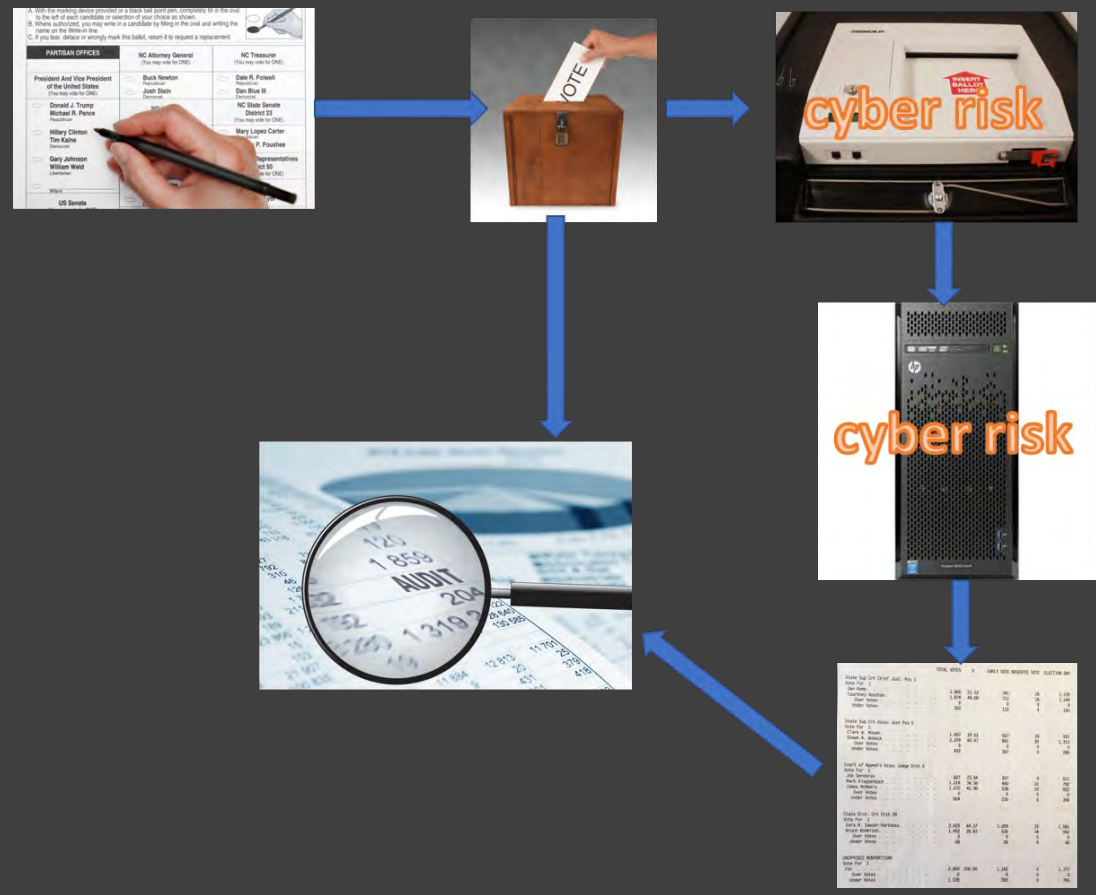
Assurance: How the public gains confidence in such a system

- Understand threats
- Reduce sources of risk (more computers = more risk)
- Manage vulnerabilities
- Explain what happens when there is a failure

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

What does a resilient election system look like?

- Only allows essential computer technology
  - Voter registration
  - Vote tabulation
  - Appropriate accommodation for disabled voters
- Applies NIST cybersecurity profiles to all computerized components
- Avoids single points of failure
- Subjected to end-to-end penetration tests
- Imposes no intermediate steps between record of voter intent and electronic tabulation of vote totals
- Focuses on physical security and chain of custody of cast ballots
- Implements statistically valid post-election audits to reconcile
  - Securely archived hand-marked paper ballots
  - Electronically tallied vote totals




Thank you