

# Some Key ways to Make Elections More Trustworthy

[ElectionSec.org](http://ElectionSec.org)

# Eric Lazarus

- I am the founder of ElectionSec.org.
- Researcher since 2005.
- Developer of threat models
- Co-developer of SOBA
- Honored to advise Conservative Republican Alliance of NY

# Some questions

- Tell me about [freedom515.com](http://freedom515.com) and your own goals

# **VOTERS BILL OF RIGHTS**

# Indelible Record of the Voters' Choices

- Hand marked paper ballots are a great technology:
  - Counted/recounted
  - If machines break, people can still vote on them
- Disabled people have other needs

# Public and Transparent Post Election Audits

- All election contests (i.e., races) must be audited in a statistically, valid, public, transparent way so that American voters are not forced to trust technology to capture and tabulate the vote. Instead, we should trust human eyes and witnesses.
- These audits should be carried out in a participative way.

# Secure and Transparent Ballot Handling

- The security of those ballots and the transparency with which they are handled and stored, must be treated as a national security priority.
- For example, it is generally good practice for pairs of poll workers to transport the voted ballots from the polling places to the election warehouse.
- It is not as good, to have police come and pick up ballots from many polling places.

# Transparency of Election Operation Processes

- Manual published in advance
- Numbered vests and hats
- Make observation meaningful



# The Security of Absentee Ballots

- Intelligence mail bar codes
- Exploring an app / one-time password (OTP)

# freedom515.com could join with Conservative Republican Alliance of NY

## [Conservative Republican Alliance of NY](#)

- Working on a Voter's Bill of Rights and looking to work across the isle.

**WHAT IS SOBA?**

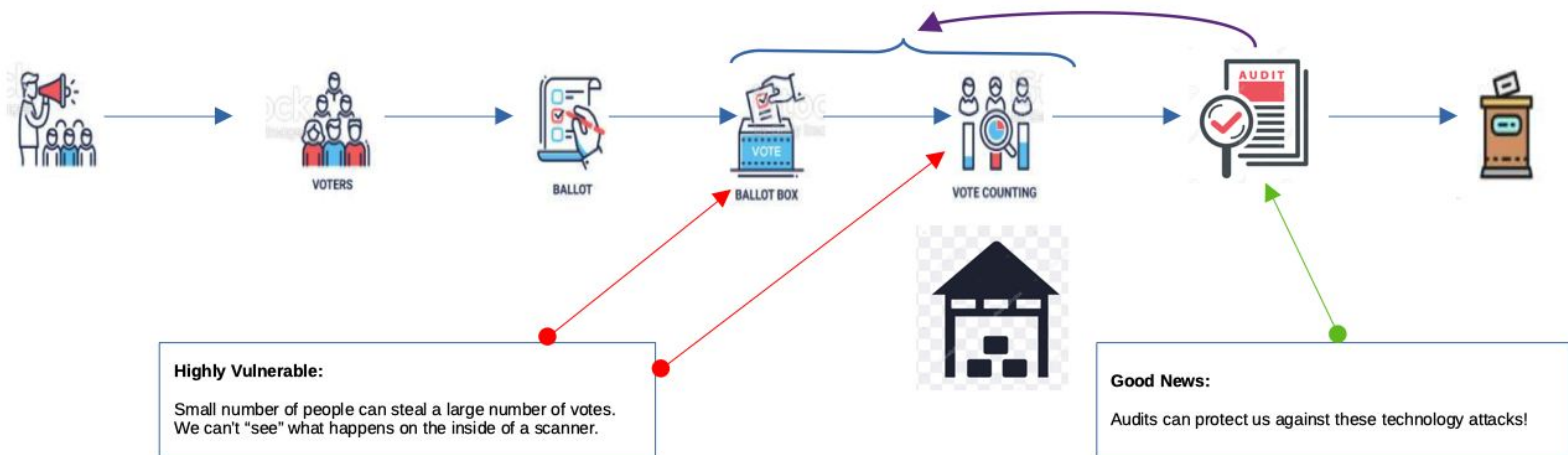
# We know what to do about attacks on voting machines!

All Good Security is Holistic

Resilient against errors and malevolence

Resilient against unfair disparaging attacks

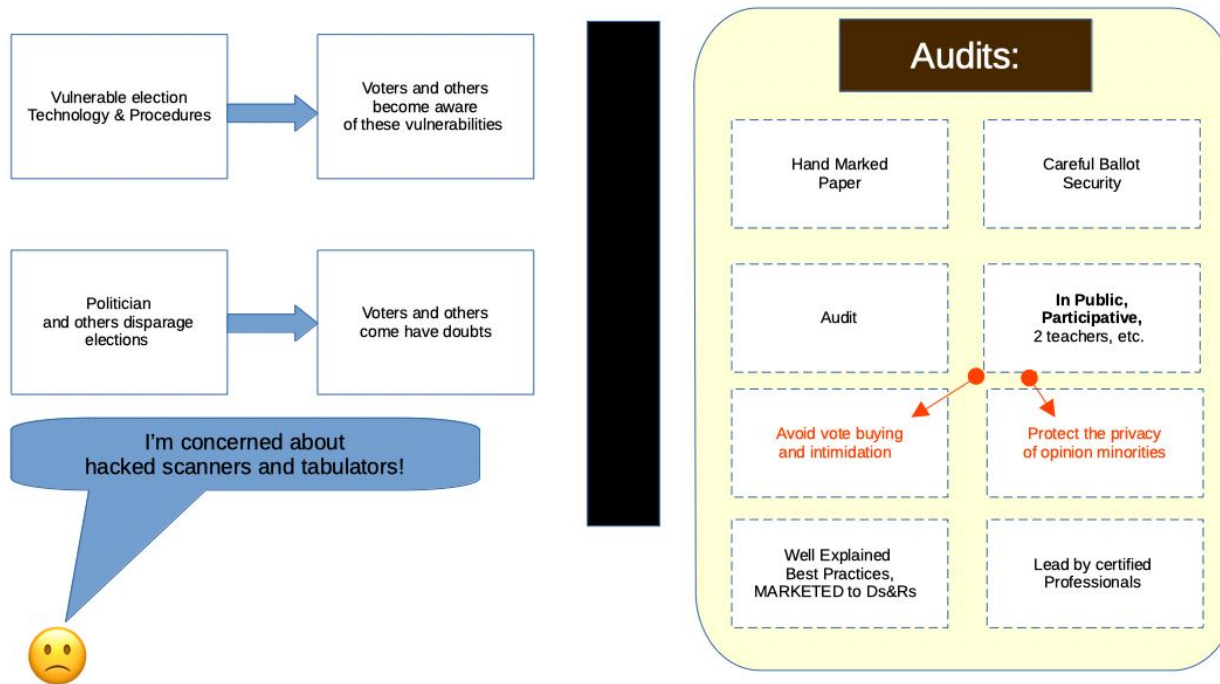
bipartisan **Select Committee on Intelligence United States Senate:**  
We are under attack from a well resourced foe!



Attacks on voting terminals and tabulators are scary but we know what to do about them.

# A Best Practice Audit should block both

How can we do better? Part of the answer involves best-practice audits:



A best-practices audit blocks inaccuracy and, we hope, the perception of inaccuracy.

# Thought Experiment: “The Audit Game”

BALLOT IDENTIFICATION		CONTEST	
PRECINCT (BOX)	ORDER IN BOX	GOVERNOR	MAYOR
1	1	BUGS BUNNY	MINNIE MOUSE
1	2	PORKY PIG	WILE E. COYOTE
1	3	BUGS BUNNY	WILE E. COYOTE
1	4	BUGS BUNNY	WILE E. COYOTE
1	5	PORKY PIG	MINNIE MOUSE
1	6	BUGS BUNNY	WILE E. COYOTE
1	7	BUGS BUNNY	WILE E. COYOTE
1	8	PORKY PIG	MINNIE MOUSE
1	9	BUGS BUNNY	WILE E. COYOTE
1	10	BUGS BUNNY	WILE E. COYOTE
2	1	BUGS BUNNY	WILE E. COYOTE
2	2	BUGS BUNNY	WILE E. COYOTE
2	3	BUGS BUNNY	MINNIE MOUSE
2	4	BUGS BUNNY	WILE E. COYOTE
2	5	PORKY PIG	MINNIE MOUSE
2	6	BUGS BUNNY	WILE E. COYOTE
2	7	BUGS BUNNY	MINNIE MOUSE
2	8	PORKY PIG	MINNIE MOUSE
2	9	BUGS BUNNY	WILE E. COYOTE
2	10	BUGS BUNNY	WILE E. COYOTE

The tabulator is saying that box2, Ballot 3 has a vote for bugs and Mini. But is it True?

What a player gets in the “Audit Game”, full “Cast Vote Records” designed to be loaded into a spreadsheet or the like.

# SOBA

BALLOTS	
BALLOT IDENTIFICATION	
PRECINCT (BOX)	ORDER IN BOX
1	1
1	2
1	3
1	4
1	5
1	6
1	7
1	8
1	9
1	10
2	1
2	2
2	3
2	4
2	5
2	6

There are 10 ballots in box one. Not publishing what votes are on them.

Ballots, as an Audit Participant gets in a SOBA Audit.

# SOBA

DISAGGREGATED VOTES		
CONTEST	VOTE	BALLOT COMMITMENT
GOVERNOR	BUGS BUNNY	186005FEA2F69
GOVERNOR	PORKY PIG	48F8B92BAB
GOVERNOR	BUGS BUNNY	4BD74CF4C9728DF
GOVERNOR	BUGS BUNNY	1CBCACA037C3
MAYOR	MINNIE MOUSE	7732FAF0062
MAYOR	WILE E. COYOTE	10102F9A9961B24
MAYOR	WILE E. COYOTE	066A0629446FE
MAYOR	WILE E. COYOTE	54BF6BC3B585CE
MAYOR	MINNIE MOUSE	DDA8982B4643

Someone voted for wile and we can tell you which ballot this vote is from if that ballot is selected.

Disaggregated votes, as an Audit Participant gets in a SOBA Audit.



# SOBA

## What is cryptographic commitment?

A **cryptology hash function** takes an arbitrary data set and provides a fixed length "**fingerprint**" designed to make it hard for you to find another dataset that would "hash" to the same value



Unique fixed length "name" for the arbitrary length data.

We commit the ballot ID for each disaggregated vote so that later we can prove which ballot that vote came from.



```
% echo "precinct=12,ballot=4321,salt=972386123783489136023213324" > file.txt  
% shasum --algorithm 256 file.txt  
e2db61a36d8e64b8afce3b5cc8b8e45061471dfe8d98ee76cfd5c5ca82515bd7 file.txt
```

## What is Cryptographic Commitment?

**CONCLUSION**

# SOBA Shows us:

- It is possible to make an auditing process that is public and privacy preserving
- Is it what you want?