SMU | LYLE SCHOOL OF ENGINEERING

U.S. Election Security System

SMU | LYLE SCHOOL OF ENGINEERING

Scope of Project

Our team hopes to develop a solution to the election fraud and hacks that occurred in the 2016 Presidential election due to cyber security hacks and outdated voting software. Thus, we have developed a list of questions for the Secretary of Homeland Security to clarify the requirements of the new system and will conduct conceptual, preliminary, and detailed designs to come to the best system alternative that fits within the given budget and timeline. The system will then be tested so that it can be used for upcoming midterm, presidential, and other local elections.

SMU | LYLE SCHOOL OF ENGINEERING

Stakeholder Analysis – U.S. Election Security

Primary Stakeholder: Secretary of Homeland Security

Their mission is to protect the safety of U.S. citizens, under the DHS. As the top official of the U.S. Department of Homeland Security, the Secretary handles domestic and foreign threats, natural disasters, and immigration issues. Election fraud and international hacks fall under the scope of the Secretary of Homeland Security's responsibilities.

Secondary stakeholders include the National Security Advisor, Director of the FBI, technical support teams/engineers, and end-users.

1. What eligibility qualifications does a voter need to have to legally vote in an electronic voting system?
2. What is a higher priority: increased cyber security against foreign hacks or updating outdated electronic voting systems in all states?
3. What is the timeframe that the new election system needs to be implemented? What are the performance measures at each stage of development?
4. How often should audits be conducted on the electronic voting software?
5. Will this voting system only be used for presidential elections or primaries, midterms, etc?
6. How long does private voter information needed to be securely stored in the computer system? Should the storage system be Cloud-based?
7. Does the new electronic system need to have artificial intelligence capabilities to ensure voter impersonation doesn't occur at the polls?
8. What past firewall systems are in place and do we have access to them?
9. What legal entities or engineering departments are available for providing specifications and technical support?
10. Will end-users (citizens) or a team of super users test the new system? What network will the secure system be tested on?
11. Will the new electronic voting system require a paper trail as a backup or can all data be stored on the system?
12. Should the new security system's scope extend to monitoring social media and news outlets to prevent the spread of false information or foreign malicious messages?
13. What should the user interface look like?
14. What capabilities need to be put in place to account for disabled voters?
15. Should voters receive a receipt confirming their vote?
16. Which method is better for election security, an electronic voting system or a paper ballot?
17. What is the timeframe that votes are processed and counted?
18. How should vote counting be audited for manipulation?

SMU | LYLE SCHOOL OF ENGINEERING

High Level Requirements

1.0 Provide a variety of ballot formats to maximize voter turnout
- 1.1 Provide paper ballots at locations that do not have access to updated electronic voting systems
  - 1.1.1 Paper ballots must be filled out in a secured area and placed in a confidential envelope
  - 1.1.2 Paper ballots must only be seen by counting officials when votes are being tallied
- 1.2 Use public network direct recording electronic voting system/kiosk as primary method of collecting votes
- 1.3 Provide provisional ballots for absentee voters or if system issue arises

2.0 Issue receipt to voters immediately after ballot is submitted
- 2.1 Issue electronic receipt via email for electronic voters
  - 2.1.1 Have the option to print a receipt on-site from the voting machine
- 2.2 Receive a ballot receipt if filling out a physical form in-person from an administrator
- 2.3 Receive a receipt via email or mail if submitting an absentee ballot

3.0 Allow voters to review vote electronically before submitting final ballot
- 3.1. Voters should be able to return to previous pages when filling out ballot electronically
  - 3.1.1 Voters should be able to easily change their selections via touch screen
- 3.2 Voters should be able to view their complete ballot summary before submitting it

4.0 Make electronic user interface easy to read and operate
- 4.1. Use large text size and bold the names of candidates
  - 4.1.1.Have braille and larger text size options for special needs voters
- 4.2. Enable touch screen technology
- 4.3 Have language options in English, Spanish, Chinese, and Hindi

5.0 Store voter data securely
- 5.1 Voting data should be recorded in a removable memory component
- 5.2 Store a printed copy of ballots in an encrypted local data system
- 5.3 Consolidate vote totals to a secure central location/data system in each state

6.0 Authenticate voter identity to verify eligibility
- 6.1. Require valid driver's license or passport at polling location
- 6.2. Use artificial intelligence to recognize a voter based on a fingerprint or facial scan
  - 6.2.1 Use driver's license or passport image stored in government

database for facial recognition

7.0 Audit votes to detect fraud
- 7.1 Conduct audits before and after elections, at least once a year
  - 7.1.1 Compare paper votes and electronic votes using a random sample of voting districts in each state
- 7.2 Review past voting receipts to verify if they match vote totals

8.0 Count votes in a timely manner
- 8.1 Allow all votes to come in within a 12 hour grace period
- 8.2 Count votes within 36 hours of the final polling day
  - 8.2.1 Compile paper, provisional, and electronic ballots in each state
  - 8.2.2 Perform at least two final counts for accuracy

9.0 Compile voter registration forms
- 9.1. Have voter registration forms accessible in local database so operators can verify they are complete at polling locations
  - 9.1.1 Update system continuously to account for incoming voter registrations, up until the voter registration deadline
- 9.2 Grant access in each state to view other states' voter registrations, to check if someone is registered in a different state

10.0 Accommodate voters with disabilities
- 10.1 Have at least 2 disability accommodation kiosks
  - 10.1.1 Allow the use of approved headphones and foot pedals with a government-issued notice
- 10.2 Allow wheelchair access at each polling location

11.0 Store voter data in records
- 11.1 Store voter data until 10 years after the death of the voter or 20 years after their last vote if not listed as dead
- 11.2 Store data in a local system that is not Cloud-based
  - 11.2.1 Have paper copies stored as backups at a central location in each state

12.0 Test electronic voting system
- 12.1 Create a new private network for initial testing
  - 12.1.1 Use a team of super-users to perform regression and user acceptance testing
- 12.2 Move onto general population testing once super-users are satisfied

13.0 Prevent voters from voting multiple times
- 13.1 Upon submission, issue each voter a unique ID number to prevent them from voting twice

13.1.1 Make this voting ID accessible to all states' polling locations
13.1.2 Voter ID expires after each election

14.0 Implement cyber security system to prevent hacks
14.1 Lock votes after submission so they cannot be changed or accessed until Counting
14.2 Encrypt voting data so voter identity remains anonymous
14.3 Enable firewalls to prevent foreign interference

15.0 Properly screen software developers, operators, and maintenance attendants
15.1 Conduct thorough background checks on all personnel who handle electronic voting system
15.1.1 Check if they are U.S. citizens and are over the age of 18
15.1.2. Check if they have strong involvements in a political party or a history of collusion
15.2 Grant limited access to voting data and system controls

16.0 Distribute authority among multiple administrators
16.1 Administrators may only operate at one polling location in one state
16.2 Administrators need to have a supervisor to audit their performance
16.3 At least two administrators need to be on premise at each polling location

17.0 Prohibit the use of personal electronics during voting
17.1 Restrict the use of cell phones, cameras, smart technology, recording devices at polling locations
17.1.1 Require that personal electronics be handed in before approaching the ballot and returned once ballot is submitted
17.1.2 Photos may only be taken outside the polling location

18.0 Ensure there are enough electronic voting machines at each polling location
18.1 Have at least 4 electronic voting machines at each location
18.2 Have at least 1 administrator for every 2 machines
18.3 Ensure each polling location has sufficient parking

19.0 Select polling locations in highly frequented areas with access to all demographics
19.1 Place electronic voting systems in schools, libraries, office buildings, government buildings, and senior homes
19.1.1 If polling location is not government-affiliated, conduct background
checks on volunteers
19.1.2 Make sure there are CCTV cameras on-site
19.2 Have at least 4 polling locations per county

20.0 Restrict access to vote counting

20.1 Do not allow personnel involved in development, maintenance, or ballot administration to count votes

20.1.1 Recruit approved counters who have had no visibility to voting data during polling

21.0 Have the option of straight-ticket voting

21.1 Include an option in the corner of the kiosk screen to select all candidates from one party on an electronic ballot

21.1.1 Before submission, have a message appear that asks users to confirm their straight-ticket

22.0 Provide an unbiased blurb about each candidate so voters are educated and more likely to vote for all positions

22.1 Include a blurb about each candidates' platform, when clicked, on the kiosk so voters can compare candidates

23.0 Account for network/power/system failures

23.1 Have paper ballots at each electronic voting location in the case of a system failure

24.0 Limit the hours operators and voters have access to the kiosks

24.1 Do not operate kiosks outside allotted polling hours

24.2 Lock systems during off-times so people cannot access them or vote Illegitimately

24.3 Require a password to unlock the systems inside regular polling hours

25.0 Partner with ride-share service to give rides to polling locations

25.1 Market to voters more than 50 miles away from a polling location in each County

25.1.1 Provide the offer via email

25.2 Offer rides to polling locations during early voting as well

26.0 Summarize key statistics to news outlets

26.1 After votes have been counted, provide key statistics, without revealing voter identities, to news outlets to report on after elections

26.1.1 Provide data on demographic, party, county, and historical trends

27.0 Count votes after final polling is complete

27.1 Do not count votes before the final election day

27.2 Do not allow vote totals to be disclosed until all votes have been collected

28.0 Require voter signature before submitting ballot

28.1 Before an electronic vote is submitted, ask for a signature via touch screen

for voters to sign

28.1.1 Store the electronic signature with a copy of the ballot in local storage system

28.2 For paper ballots, require a physical signature

29.0 Clear electronic voting systems before they are used for another election

29.1 Remove pre-existing data and menu options from electronic voting system before they are used again

29.1.1 Electronic systems should be scrubbed within 6 months of the next election

30.0 Design kiosks so bystanders cannot see voter selections

30.1 Electronic voting systems in public areas should have screen protection so bystanders cannot see voter selections

30.1.1 Have side panes that obscure screens

30.1.2 Darken the screen so it is not visible to bystanders

31.0 Authenticate votes and protect voter data

31.1 Verify voter identity with government-issued ID and fingerprint

31.2 Check if voter is registered

31.3 Have voter sign authentication agreement before submission

SMU | LYLE SCHOOL OF ENGINEERING

Preliminary Design

Cybersecurity

Online and Physical Voter Authentication

- **1.0** Compile voter registration forms
  - **1.1** Have voter registration forms accessible in local database so operators can verify they are complete at polling locations
    - **1.1.1** Update system continuously to account for incoming voter registrations, up until the voter registration deadline has passed
    - **1.1.2** Voter data must be encrypted
  - **1.2** Grant access in each state to view other states' voter registrations, to check if someone is registered in a different state
    - **1.2.1** Access requires two-factor authentication, unique username, and password
- **2.0** Authenticate voter identity to verify eligibility
  - **2.1** Require valid driver's license or passport at polling location
  - **2.2** Use artificial intelligence (AI) to recognize a voter based on a fingerprint or facial scan
    - **2.2.1** Use driver's license or passport image stored in government database for facial recognition
- **3.0** Issue receipt to voters immediately after ballot is submitted
  - **3.1** Issue electronic receipt via email for electronic voters
    - **3.1.1** Have the option to print a receipt on-site from the voting machine
  - **3.2** Receive a ballot receipt if filling out a physical form in-person from an administrator
  - **3.3** Receive a receipt via email or mail if submitting an absentee ballot
    - **3.3.1** Have the option to select if user wants receipt and pick delivery method

Secure Voting

- **4.0** Test electronic voting system
  - **4.1** Create a new private network for initial testing
    - **4.1.1** Use a team to perform user acceptance testing
      - **4.1.1.1** Conduct regression, interoperability, and sustainability testing
  - **4.2** Move on to general population once initial testing is complete
- **5.0** Provide a variety of ballot formats
  - **5.1** Provide paper ballots at locations that do not have access to updated electronic voting systems
    - **5.1.1** Paper ballots must be filled out in a secured area and placed in a confidential envelope

- **5.1.2** Paper ballots must only be seen by counting officials when votes are being tallied
  - **5.1.2.1** Paper ballots must be stored in secure lockbox until counting
- **5.2** Use Direct Recording Electronic Voting System kiosk as primary method of collecting votes
- **5.3** Provide provisional ballots for absentee voters or if system issues arise

6.0 Properly screen software developers, operators and attendants
- **6.1** Conduct thorough background checks on all personnel who interact with electronic voting system
  - **6.1.1** Check if they are U.S. citizens over the age of 18
  - **6.1.2** Check if they have strong affiliations with a particular political party or have a history of collusion
- **6.2** Grant only compartmentalized access to voting data and system controls

7.0 Distribute authority among multiple administrators
- **7.1** Administrators may only operate at one polling location in one state
- **7.2** Administrators need to have a supervisor to audit their performance
- **7.3** At least two administrators need to be on premise at each polling location

8.0 Prohibit the use of personal electronics during voting
- **8.1** Restrict the use of cell phones, cameras and other recording devices at polling stations
  - **8.1.1** Require that personal electronics be handed in or left in the car before approaching the kiosk
  - **8.1.2** Photos may be taken only outside of the polling station

9.0 Segregation of duties to restrict access to vote counting
- **9.1** Do not allow personnel involved in software development, maintenance or ballot administration to count votes
  - **9.1.1** Recruit approved counters who have had no visibility to anything other than the ballots they count

10.0 Limit the hours that operators and voters have access to the kiosks
- **10.1** Do not operate kiosks outside of pre-determined polling hours
- **10.2** Lock systems during off-hours to ensure people cannot access them
  - **10.2.1** Require a password to unlock the systems within regular polling hours

11.0 Require voter signature before submitting ballots
- **11.1** Before an electronic ballot can be submitted, require a signature via touch screen for voters to sign
  - **11.1.1** Store the electronic signature with a copy of the ballot in the local DBMS
- **11.2** For paper ballots, require a physical signature

12.0 Design kiosks so that bystanders cannot see voter selections
- **12.1** Electronic voting systems shall have screen protections to prevent bystanders from seeing the voter selections of others
  - **12.1.1** Have side panels that obscure screens

12.1.2 Set screen to low contrast to prevent visibility to passersby

Data Protection

13.0 Comply with all requirements of the General Data Protection Regulation (GDPR)
- **13.1** Provide voters with statutory service
  - **13.1.1** Remain within governmental statutes and regulations
- **13.2** Record details about voters in accordance with the law
  - **13.2.1** Collect details such as name, address, date of birth and nationality
  - **13.2.2** Allow for scanned application forms
  - **13.2.3** Require signature for postal vote checking
- **13.3** Keep voter records in accordance with legal obligations and in line with statutory retention periods
- **13.4** Share voter records
  - **13.4.1** Share only if law requires where formal court order has been issued
  - **13.4.2** Share only if necessary to perform a task of public interest

14.0 Allow voters to review vote electronically before submitting final ballot
- **14.1** Voters should be able to return to previous pages when filling out ballot electronically
  - **14.1.1** Provide easy-to-see navigation buttons
- **14.2** Voters should be able to easily change their selections via touch screen
  - **14.2.1** Provide easy-to-use selection options
- **14.3** Voters should be able to view their complete ballot summary before submitting it
  - **14.3.1** Display all choices for accurate reference

15.0 Store voter data securely
- **15.1** Voting data should be recorded in a removable memory component
  - **15.1.1** Utilize single use DVD/CD
  - **15.1.2** Use single use, disposable, removable USB thumb drive
  - **15.1.3** Use re-formatted, multi-use removable USB thumb drive
- **15.2** Store a printed copy of ballots in an encrypted local Database Management System (DBMS)
  - **15.2.1** Use tamper-resistant or tamper-evident seals and logs to detect any unauthorized access
  - **15.2.2** Create and maintain an inventory of storage components at each location
- **15.3** Consolidate vote totals to a secure central Database Management System (DBMS) in each state

- **15.3.1** Implement chain-of-custody utilizing two or more individuals to perform a check and verification check whenever a transfer of custody takes place
- **15.3.2** Record the names of individuals who transport the voting system equipment and materials from local sites to consolidation site

16.0 Store voter data in records

- **16.1** Store voter data until 10 years after the death of the voter or 20 years after their last vote if not listed as dead
  - **16.1.1** Minimum of two duplicates of electronic data must be retained, labeled and stored
  - **16.1.2** Store in a secure manner where any opening can be detected
  - **16.1.3** Place each duplicate separately in locked areas with restricted access
- **16.2** Store data in a local DBMS that is not cloud-based
  - **16.2.1** Have paper copies stored as backups at a central location in each state

17.0 Prevent voters from voting multiple times

- **17.1** Issue each voter a unique ID number to prevent them from voting twice
  - **17.1.1** Make this unique ID accessible to polling stations in all states
  - **17.1.2** Unique ID expires after assignee's voting session is submitted

18.0 Implement cyber security system to prevent hacks

- **18.1** Lock votes after submission so they cannot be changed/accessed until counting
  - **18.1.1** Print full copy of central accumulator's audit log after tabulation of election results
  - **18.1.2** Retain printed copy of the log with elections records for the preservation period
- **18.2** Encrypt voting data so voter identity remains anonymous
  - **18.2.1** Change encryption keys and passwords at the discretion of the general custodian of election records
  - **18.2.2** Access should be witnessed by one or more individuals who are authorized
- **18.3** Enable firewalls to prevent foreign interference
  - **18.3.1** Validate that the software being installed and used on the voting system is the same software that was certified during acceptance testing

19.0 Account for network, power or system failures

- **19.1** Have paper ballots at each electronic voting location in case of any failure
  - **19.1.1** Require manual count of paper ballots

19.1.2 Lock and secure paper ballots

19.2 Utilize non-volatile data storage

19.2.1 Recording can be done mechanically, magnetically, or optically

20.0 Clear electronic voting systems before they are used for another election

20.1 Remove any pre-existing data and menu options from electronic voting system prior to reallocation

20.1.1 Scrub electronic systems within six months of next election

SMU | LYLE SCHOOL OF ENGINEERING

Detailed Design

Cybersecurity

Secure Voting

4.0 Test electronic voting system

4.1 Create a new private network for initial testing

4.1.1 Use a team to perform user acceptance testing

4.1.1.1 Form qualified user acceptance test team

4.1.2 Select a sample population to do the initial test

4.1.2.1 Hire low-wage person to test perform regression, interoperability, and sustainability tests

4.2 Move on to general population once initial testing is complete

4.2.1 Promote the new electronic voting system in next election to get real user data and feedback

4.2.1.1 Television advertising

4.2.1.2 Newspaper advertising

4.2.1.3 Social Media advertising

4.2.1.4 Pitch meetings to DHS

5.0 Provide a variety of ballot formats

5.1 Provide paper ballots at locations that do not have access to updated electronic voting systems

5.1.1 Paper ballots must be filled out in a secured area and placed in a confidential envelope

5.1.1.1 Form paper ballots department to oversee security measures

5.1.1.2 Purchase tamper-proof lockbox to store paper ballots until counting

5.1.1.2.1 Password-protect the lockbox and build it out of dent-resistant steel

5.1.2 Paper ballots must only be seen by counting officials when votes are being tallied

5.1.2.1 Confidentiality agreement

5.1.2.2 Armed Police

5.2 Use Direct Recording Electronic Voting System kiosk as primary method of collecting votes

5.2.1 Conduct availability testing on Direct Recording Electronic Voting System

5.2.1.1 Direct Recording Electronic Voting System

5.3 Provide provisional ballots for absentee voters or if system issues arise

5.3.1 Create database for provisional ballots and absentee voters

5.3.1.1 DBMS Access

5.3.2 Store paper provisional ballots station in a secured, central area in each county

5.3.2.1 Local Secured Department

5.3.2.2 Guarded Storage

6.0 Properly screen software developers, operators and attendants

6.1 Conduct thorough background checks on all personnel who interact with electronic voting system

6.1.1 Check if they are U.S. citizens over the age of 18

6.1.1.1 Form special investigation department for background checks and monitoring of suspicious activity

6.1.1.1.1 Special Investigation Department

6.1.2 Check if they have strong affiliations with a particular political party or have a history of collusion

6.1.2.1 Special Investigation Department

6.2 Grant only compartmentalized access to voting data and system controls

6.2.1 People must not have both access of voting data and system controls.

6.2.1.1 Assign every employee a unique ID to one certain area of system

6.2.1.2 Set different login interface for voter database

6.2.1.3 Store voter data locally on a physical server

6.2.1.4 Locally stored data accessible only by approved personnel and the password is protected

7.0 Distribute authority among multiple administrators

7.1 Administrators may only operate at one polling location in one state

7.1.1 Set up a resources department that staffs poll operators

7.2 Administrators need to have a supervisor to audit their performance

7.2.1 Require annual performance evaluation by supervisor

7.2.1.1 Performance Evaluation System

7.3 At least two administrators need to be on premise at each polling location

8.0 Prohibit the use of personal electronics during voting

8.1 Restrict the use of cell phones, cameras and other recording devices at polling stations

8.1.1 Require that personal electronics be handed in or left in the car before approaching the kiosk

8.1.1.1 Have electric device detector at the door of each poll

8.1.1.2 Provide free, secure temporary lockers outside the

polling place
8.1.2 Photos may be taken only outside of the polling station
8.1.2.1 Have security guard outside each polling place enforcing this

9.0 Segregation of duties to restrict access to vote counting
9.1 Do not allow personnel involved in software development, maintenance or ballot administration to count votes
9.1.1 Recruit approved counters who have had no visibility to anything other than the ballots they count
9.1.1.1 Set up software program to monitor account activity

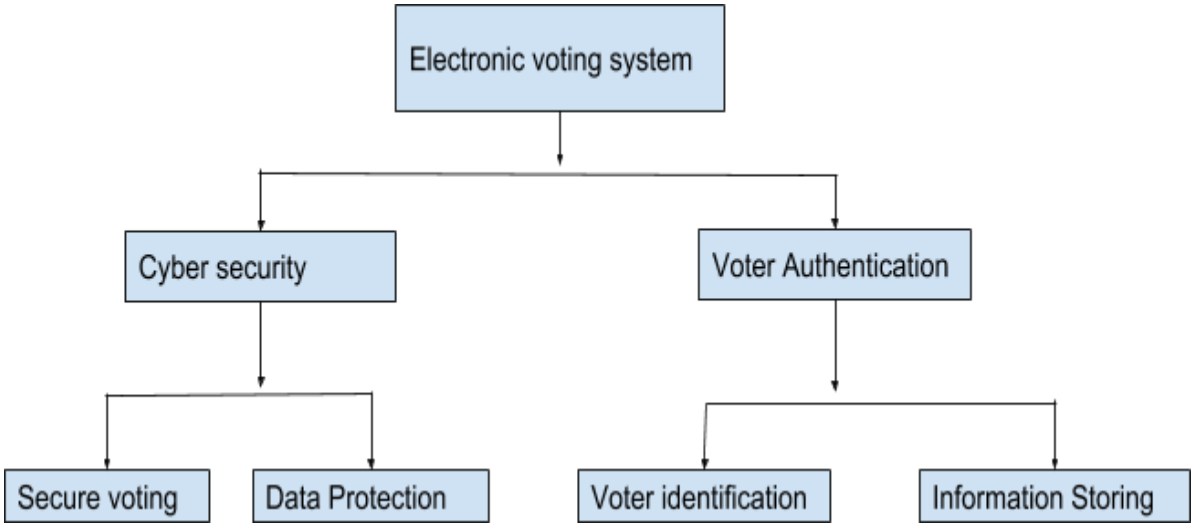
10.0 Limit the hours that operators and voters have access to the kiosks
10.1 Do not operate kiosks outside of pre-determined polling hours
10.1.1 Hire security guards for after hours surveillance
10.1.1.1 Security Guards
10.1.2 Set up security camera to monitor the station to prevent people enter the station after polling hours
10.1.2.1 Security Cameras
10.2 Lock online systems during off-hours to ensure people cannot access them
10.2.1 Require a password to unlock the systems within regular polling hours
10.2.1.2 Record a log of time and person each time system unlocks

11.0 Require voter signature before submitting ballots
11.1 Before an electronic ballot can be submitted, require a signature via touch screen for voters to sign
11.1.1 Store the electronic signature with a copy of the ballot in the local DBMS
11.1.1.1 Local DBMS Access
11.2 For paper ballots, require a physical signature
11.2.1 Store the signature with a copy of the ballot in the local secured department.
11.2.1.1 Local secured department
11.2.1.2 Guarded Storage

12.0 Design kiosks so that bystanders cannot see voter selections
12.1 Electronic voting systems shall have screen protections to prevent bystanders from seeing the voter selections of others
12.1.1 Have side panels that obscure screens
12.1.1.1 Side Panels around the screens
12.1.2 Set screen to low contrast to prevent visibility to passersby
12.1.1.2 Brightness Control Button

Test and Validation Plan

System Decomposition



Based on the detailed design, a database management system is the best means for maintaining cybersecurity and data protection measures. Compartmentalized access versus granted access based on background checks is a better option for granting employees access to voter authentication system. Kiosks should also be built with privacy screens built in physically.

Detailed Design Error:

Cybersecurity

Data Protection

- If the data is stored in physical servers then it's easy to be hacked, so there should be multiple firewalls to build protection. Data should be encrypted and password protected
- Firewalls can restrict authorized users
- Broadband to access the internet that cannot be prevented by a firewall, hence the system should be designed to be capable as an offline system
- The design does not include any backup for power or system failure. It should include a power backup and the system should be built independently from other components so it does not affect the overall system
- If the voters are doing a paper ballot, then they should scan their vote in the system and within a certain time period it will log them out if there is some stand by time to prevent voter fraud

Voter Authentication

Voter identification

- Authenticate voter identity to verify eligibility
- When arriving to the voting site the person must identify him or herself with a security officer and proper ID.
- The AI scanner first scans the right fingerprints of the user. Next, the AI scans the left hand
- The AI compares this information against the government citizen database
- The AI scans the eyes of the user and proceed with the verification against the government database
- If the retinal scan match and the fingerprints as well then the user is approved
- The user is allowed to vote
- Otherwise, if the retinal and fingerprints don't match the user must be charged a penalty fee and if necessary proceed to an investigation

Information Storing

- Set up a digital database where all citizens are registered and clearly identified.
- Record voting information from all citizens when electoral day comes in.
- Store voter's activity and information within 3 electoral periods.
- If there's no activity, don't eliminate his or her information after making sure what is the current status of this person.
- If there's activity keep storing this information within a period of 5 electoral periods as a backup.
- After this time information can be debugged.
- Information must be physically archived as well within this period of time in electoral diaries.

Type 2 Testing

Subsystem: Voter Authentication
Component: Voter Identification

- Artificial intelligence first scans the right fingerprints.
- Artificial intelligence then scans the left fingerprints.
- It compares the information to the government citizen database.
- Artificial intelligence scans the eyes.
- Verifies with the government database.
- When retinal scan and fingerprint matches, then the user is approved.
- User is allowed to vote.
- When retinal scan and fingerprint doesn't match, user is not approved.
- Penalty fee for the user who isn't approved and proceed to investigate.

TEST	EXPECTED RESULT
Fingerprint matches	Allowed to vote
Finger print doesn't match	Penalty fee/ further investigation/not allowed to vote
Retinal scan match	Allowed to vote
Retinal scan doesn’t match	Penalty fee/further investigation/not allowed to vote
If User approved	Allowed to vote
If User not approved	Penalty fee / Further investigation

TEST 3 (Partial)

STEP	VARIABLES
User arrives	Arrival demand rate
User identifies him/herself with personnel	Voter’s ID Voter’s address Voter’s citizen number
Voter’s proceed to AI scan	
AI scan verifies voter’s information against government database	Message type Message content
AI determines if user can or not vote	Covered in type 2
User is marked with a seal to identify he/she already vote	
User leaves the voting booth	
Outputs	Does the user vote? Time the user spends on voting booth

Tools for testing:

1. Functionize Software: It tests the systems quickly and efficiently. It’s one of the automation tools based on Artificial Intelligence.
2. MATLAB: For queueing simulation to get actual voter statistics and see if bottlenecks occur when using at polling places.

3. MS Excel: Used for economic analysis to see which alternatives fits within the budget.
4. Conduct regression testing to ensure individual components do not disrupt other components or system functions.
5. User acceptance testing physically with a team of super users, then move on to general population testing.

Test Plan

Components that are we going to test together:

1. Cyber security and database backup
   1.1 Ensure cybersecurity measures are applied to database backup like encryption and password protection
2. Voter identification and database backup
   2.1 Fingerprint and retinal scan with national database

Components that we are testing alone:

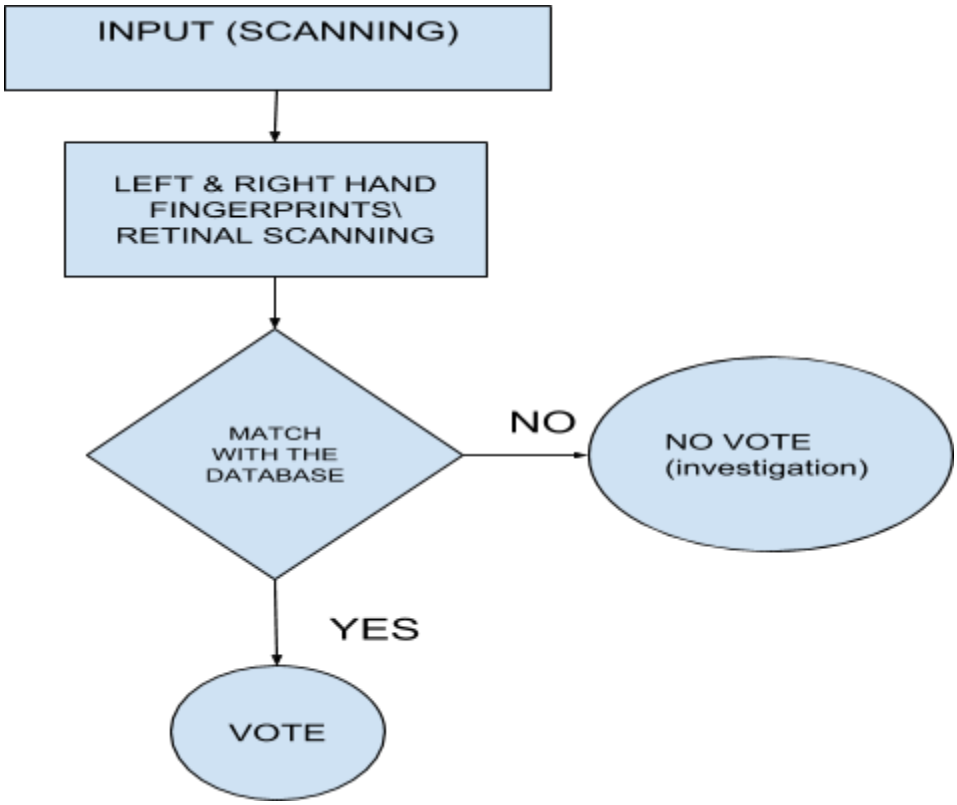
1. Physical voter identification with security officer or poll worker
2. Security of physical paper ballot lockbox
3. Usability of screen and buttons on electronic voting system

Physical testing will be conducted on the fingerprint identification system:

2. Scanning of both the fingerprints and matching them with a prototype database made for testing.
3. Scanning of the retina and match them with a prototype database system made for testing.

Virtual testing will be conducted on cybersecurity and online voter authentication systems:

1. MATLAB can be used for the virtual testing of the system with the logical functioning of the system, if the system allows to give them a vote only if there fingerprints and retinal scans matches with the database systems.


INPUT (SCANNING)
LEFT & RIGHT HAND FINGERPRINTS\ RETINAL SCANNING
MATCH WITH THE DATABASE
NO
NO VOTE (investigation)
YES
VOTE