JASTGAR e*VOTE* System Overview

"An electronic voting system to assist governments in identifying voters and their vote submissions via electronic technology."

Created by:

Alex St-Gardien Jecrois, and
Thomas Bronack

Alex St-Gardien Jecrois, JASTGAR, Pres. and CEO ajecrois@Hotmail.com

Thomas Bronack JASTGAR, EVP and CIO bronackt@gmail.com

5/20/2016 JASTGAR e*Vote* System 1

The JASTGAR e***VOTE*** electronic voting system was designed to address voting system problems related to Fraud and Corruption and to guaranty "**One Person – One Vote**".

The system is based on an ***eCARD***, which is a Personal ID Card using a person's Bio-Metrics to guaranty identity. Many ***eCARD APPs*** for Personal, Business, and Government users will be a natural offshoot of the ***eCARD***.

Through the use of our system, citizens will trust election results to provide an accurate representation of their desired direction. We also hope that this system will lead to improvements in the country's infrastructure, education, and living conditions.

Alex St-Gardien Jecrois has devoted his attention to defining the needs of the people, while Tom Bronack has performed research leading to the design of the ***eVOTE*** electronic voting system, which utilizes the latest technology to prove a person's identity and validate that they have not voted previously in this election. We also developed an ***eVETTING*** process that validates a person's identity and background, then stores the Information on a person's ***eCARD*** and within our Data Base.

Security precautions include encryption and network security, while physical security personnel at Voting Stations are warned of fraudulent activities as the criminal is still at the Voting Station, so that the criminal act can be stopped and criminal apprehended on the spot. Supportive evidence is captured, documented, and made available to support prosecution of criminals. Role Based Access Control (RBAC) is used to support our security and authorization process.

Once word of these safeguards becomes public, criminal attempts will reduce naturally and a safer election will be conducted.

JASTGAR e*VOTE* System – Overview

JASTGAR eVOTE

The JASTGAR eVOTE electronic voting system provides:

JASTGAR has designed and "**Patented**" the ***eVOTE*** electronic voting system, which will guaranty an efficient, accurate, auditable, and legal voting process that insures a person only votes once per election and results are produced and distributed in near real-time. Its features include:

- "**One Person – One Vote**" to guaranty honest elections and capture Voter Fraud and Corruption;
  - **Utilizes Bio-Metrics** to scan Finger Print, Palm Print, Eye Scan, and/or Facial Recognition,
  - "**Smart Card**" stores bio-metric data for comparison and support "**Real ID Act**",
    - **Locally Verifies Voter identity** at Voting Station,
    - **Remotely Validates** that the Voter has not voted at another location,
    - **Insures** Voter has the "**Right-to-Vote**" by checking Eligible Voters databases.
- **Fully electronic** to eliminate Paper Ballots;
- **Provides** near real-time voting calculations and displays to track voting results;
- **Accommodates** people with a disability;
- **Supports** remote locations lacking proper **electric and communications** abilities;
- **Project Plan** includes:
  - Needs Analysis, RFP Generation to selected vendors, Vendor evaluation and selection, system development, testing, acceptance, implementation, support, and maintenance,
  - Staff selection and training of local personnel.
- **Citizen awareness programs** and orientation to improve citizen / voter technology education.

Bio-Metric authentication techniques include: fingerprints; DNA; face, hand, retina, and facial features; odor, and voice analysis. Behavioral Characteristics are related to the pattern of the behavior of a person, such as typing rhythm, gait, gestures, and voice.

Perform on-line internet searches to learn more about Bio-Metrics and Behavioral Characteristics.

Real ID Act – Title II, H.R. 1268 – Emergency Supplemental Appropriations Act for Defense, The Global War on Terror, and Tsunami Relief, 2005 (Enrolled as Agreed to or Passed by Both House and Senate.

Defines requirements for a Real ID Card that can be used to verify a person is who they claim to be.

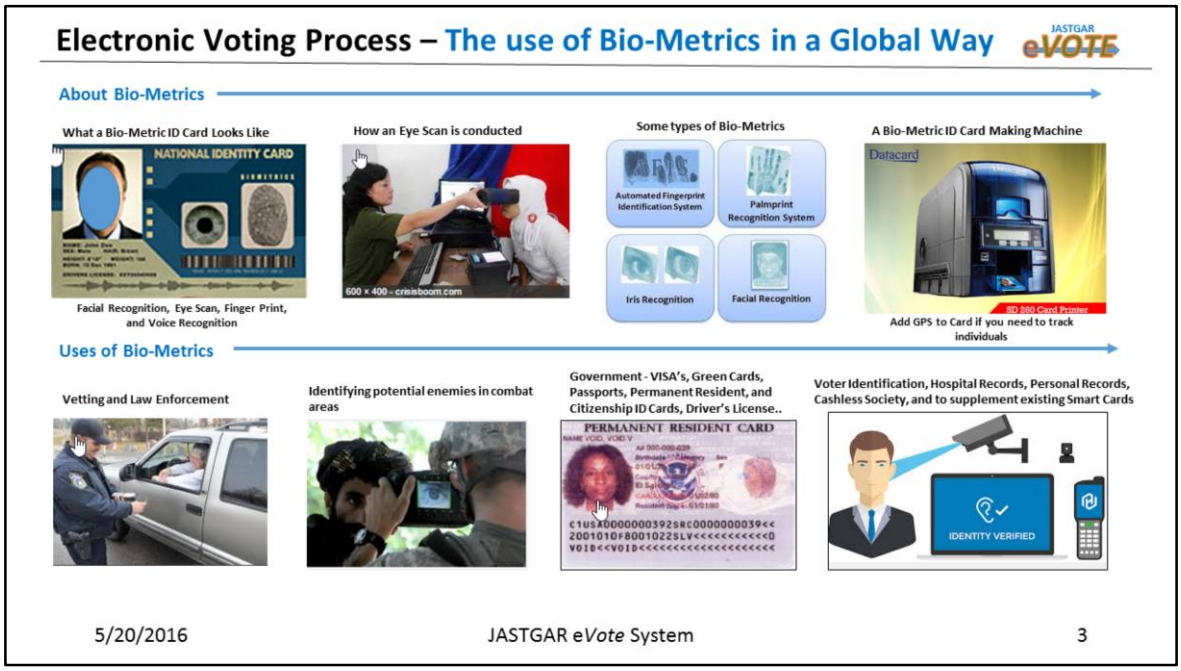
5/20/2016 JASTGAR e*Vote* System 2

The ***eVOTE*** electronic voting system has many safeguards built into it that will help a country conduct safer and more accurate elections, including:

1. **Validating Voters** entering the Voting Station by comparing their Bio-Metric signature (Eyes, Face, Finger Prints) with their Voter ID Card (Local Verification)
2. **Examining their Voting record** contained in our Voter Activity Data Base to insure that the voter has not previously voted in this election at another site.
3. **Providing the Physical Security Guard** with the Voter's Identity so that the Guard can arrest the person on the spot and hold them for questioning or prosecution.
4. The ***eVOTE*** system will produce **the documentation** needed to support prosecution including an Audit Trail of the Voter's Records and even Pictures of them voting.
5. **Provide assistance to people with disabilities**, like: Brail / Spoken Word for Blind people, or instruction displays for death people.

A **Voter's Bio-Metrics** can be stored on a Smart Card chip and the card will stay in the machine until the Voter is validated. If not, then the card will not be returned to the fraudulent voter. These safeguards will result in a truer representation of the public's desires, while reducing costs (paper elimination), speeding the production of voting results through electronic displays and reports, and improving the confidence of the population in their government.

We believe the ***eVOTE*** system will allow you to **leap-frog all current voting systems** to produce faster and more accurate voting results, while improving the knowledge base of the populace on how an understanding of electronics and computing can improve their lives.



Examples of how **Bio-Metrics** is used with Smart Cards is shown in this slide. In the top left picture, the Identity Card shows a picture, finger print, eye scan, and voice recording but those images are not needed on the outside of the card. We store that information within the chip in the ***eCARD***. To verify a person's identity, they will place their card into a reader and have their bio-metric signature scanned (eye scan, finger print, facial recognition, etc.). If a match is made, then that person will be verified, if not they will be rejected and security notified. As different uses for this information arose, it led us to define ***eCARD APPs***.

We can also perform multiple searches on the person as needed. For example, in the ***eVOTE*** voting system we check that the person is allowed to vote, that they haven't already voted at a different location, or if they have any "Wants and Warrants" for their arrest. As additional validations are made, it led us to develop the ***eVetting*** system.

We believe that the ***eCARD***, ***eCARD APPs***, ***eVOTE*** and ***eVETTING*** technologies are going to be in high demand going forward, because it is becoming increasingly more important to identify and protect personal identity. We hope to eliminate ID Theft through our approach, and may even help our society go Cashless, which would go a long way towards eliminate crimes because access to your funds would require your Bio-Metric information.

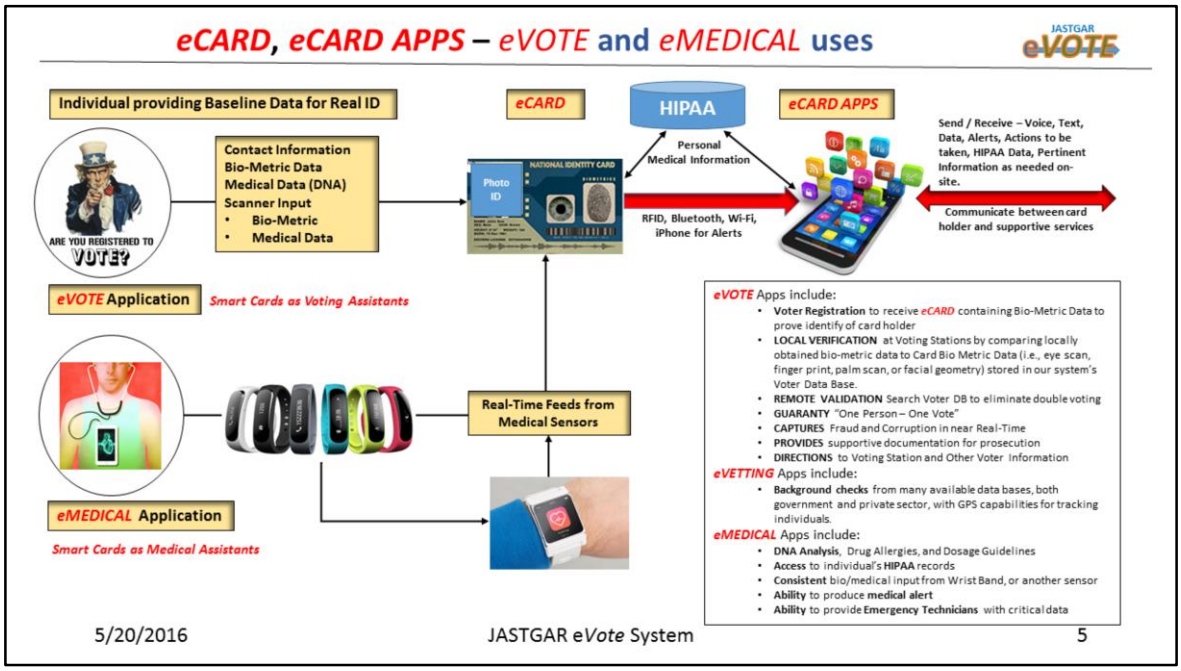
Products available through JASTGAR

- ***eCARD*** – Used to produce a Universal Smart ID Card containing an individual's bio-metric information that can be locally scanned to verify a person is who they claim to be.
- ***eCARD APPS*** – mobile smart phone applications that provides individuals with specific, and sometimes confidential, information from a hand held or PC based device.
- ***eVETTING*** – an application that utilizes a person's eCARD and available data bases to validate an individuals identity and background, so that they can be allowed access to sensitive information and locations.
- ***eVOTE*** – an electronic voting system that guaranty's "One Person – One Vote".
- ***eMEDICAL*** – an applications that can be used by an individual and the Healthcare industry to scan an individuals DNA record (within HIPAA compliance) and obtain medical recommendations and guidelines associated with dosages and treatments that can enhance an individual's medical treatment.

5/20/2016 JASTGAR e*Vote* System 4

These products are created in the following sequence:

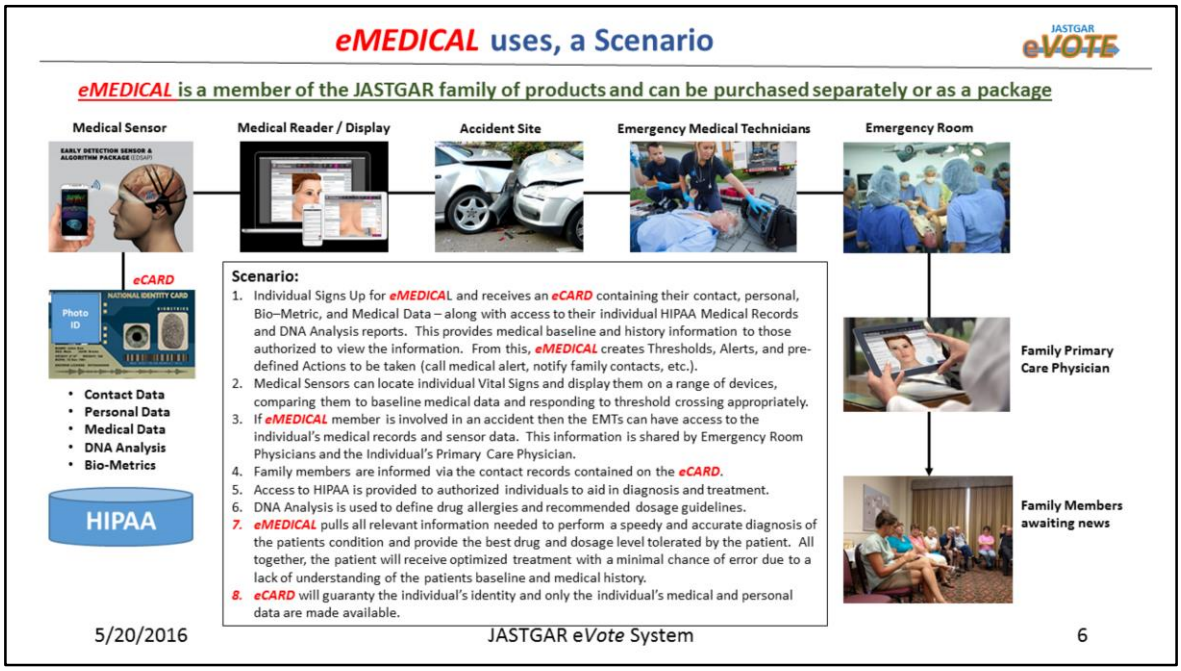
- ***eCARD*** – the foundation of the system is a means to guaranty a person's identify through the use of their bio-metric signature.
- ***eCARD APPs*** – Mobile and Server based applications that can turn an eCARD into a Universal Identification Smart Card for use by government and private sector enterprises.
- ***eVETTING*** – Used to validate a person's background that will prove invaluable to employees, law enforcement, and alien / immigration control.
- ***eVOTE*** – Used to guaranty "One Person-One Vote" by eliminating fraud and corruption from the voting process.
- ***eMEDICAL*** – Used to better protect individuals from over doses and enhance their physicians ability to treat their symptoms because of the DNA analysis contained in the card chip. Can be used by emergency medical personnel in times of crisis.



Starting with the creation of the ***eCARD***, the JASTGAR family of products includes a new addition – ***eMEDICAL***, which is an application that utilizes DNA and other medical data analysis to provide patient guidelines like drug allergies, dosage recommendations, medical history, family traits, what to monitor, how to respond, and reading real-time information from sensing devices (think Wrist Band) and comparing the information with Vital sign ranges and thresholds (i.e., Heart Beats, Blood Pressure, body temperature, etc.).

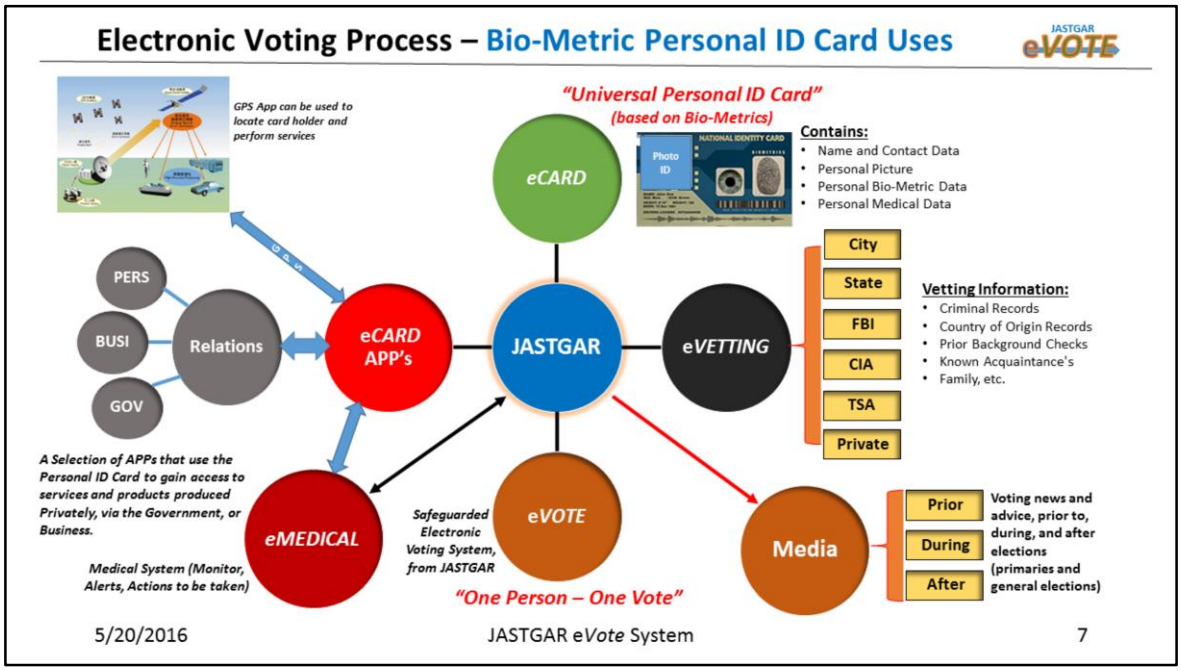
eMEDICAL will provide Emergency Medical Technicians and other medical personnel with patient information critical to providing the correct medical treatment, including:

1. Access to the patient's HIPAA file
2. Medical History, Vital Signs, Name of Family Physician, etc.
3. Who to call in case of an emergency, and many other important personal items needed by on-scene doctors and medical personnel.



Bringing all of the uses of ***eCARD*** and ***eMEDICAL*** together into a scenario like the one illustrated above would provide individuals with the best medical assistance possible by combining baseline medical and bio-metric information contained within the eCARD chip with real-time medical sensor information to monitor fluctuations crossing Thresholds (i.e., pulse rate, blood pressure, sugar level, or other indicators related to the patient's needs), initiating Alerts (medical, family, etc.), and taking pre-defined Actions to respond to a medical crisis (like a stroke, or a heart attack, or an accident like the one depicted above).

The ***eCARD*** guaranty's the person's identity and can be used to gain access to critical medical data by authorized personnel (EMT's, Emergency Room Physicians, Primary Care Physician, etc.). The ***eMEDICAL*** process will insure that medical practitioners have the information they need to quickly and accurately diagnose a patient's condition, via medical information and the DNA Analysis. ***eMEDICAL*** also provides the patients history and drug allergies, along with dosage guidelines. Through this process, the doctor / patient relationship is maintained and all relevant information needed by the physician to best diagnose and treat the patient is readily available.



JASTGAR has developed additional services that compliment the ***eVOTE*** electronic voting system including:

eCARD – a Personal ID Card based on Bio-Metrics that can be used universally, with a GPS Feature that can be used for Tracking and Locating the card holder.

***eCARD* APPs** – that can be used to perform a variety of services, like: voting, cashless transactions, receiving alerts, responding to alerts, updating personal information, and viewing the contents of the chip on your Personal ID Card, and many more possible offerings.

eVETTING – used to validate a person's identity and perform background checks

eVOTE – an electronic voting system based on bio-metric identification

eMEDICAL – To assist people with their Healthcare needs and drug dosage guidelines based on Bio-Metrics and DNA Analysis

Relations include PERS (Personal Users); BUSI (Business Users), and GOV (Government Users) who are using the ***eCARD*** and ***eCARD APPs***.

Media connections are provided through ***eVOTE*** from prior to, during, and after elections including information from the Primary and General Election. ***eCARD APPs*** can support these activities.

Electronic Voting Process – Bio-Metric Personal ID Card Benefits

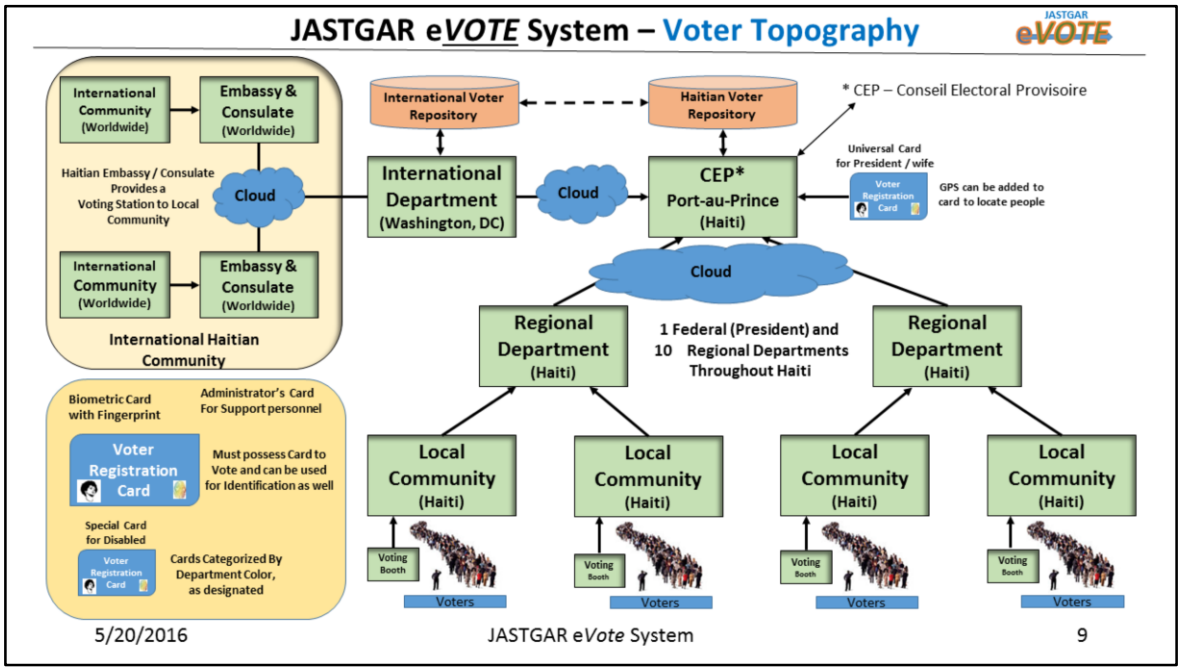
JASTGAR eVOTE

- Card contains Bio-Metric information stored in its Chip's memory, with DNA information added with *eMEDICAL*;
- Card App's can be used to examine chip data and support functions requiring identification / authorization;
- Bio-Metric Chip Information is compared with local scan to prove identity (Local ID Scans);
- Remote Validations and Second Level Checks can be conducted as required (Voting system checks if person voted at another location for this election to eliminate double voting frauds);
- Scan information can validate a person's identity in support of private services;
- One Card that serves many purposes;
- Can retain records for accounting and other services, applications, and products;
- Creates and maintains an Audit Trail that is archived to support future investigations and generate documentation needed to: capture criminal acts and assist in; identifying, apprehending, and prosecuting criminals;
- Can support a Cashless Society, or other advanced applications coming in the future;
- Can Enhance Vetting and Reduce Criminal Activity;
- Can Help Safeguard the Borders by vetting aliens seeking entry to the USA and providing a tracking *eCARD* as needed;
- Can be used to eliminate Identify Theft and a range of other criminal problems;
- Add a GPS and the card can track people as needed.

5/20/2016 JASTGAR e*Vote* System 8

This is a list of the benefits that can be derived through the use of JASTGAR products and services, which includes:

1. Identifying, tracking, and locating card holders to a level that can support Vetting.
2. Insuring "One Person – One Vote" and eliminating Voter Fraud and Corruption through ***eVOTE***.
3. Providing sufficient documentation to identify and prosecute offenders in either real-time or via archived information examination.
4. Ability to use the ***eCARD*** for a wide-range of other applications requiring positive identification of personnel to support access controls and entitlements.
5. A wide-range of ***eCARD APPS*** can be used to support other services that require in-depth identification of people (think Cashless Society, or access to Nuclear Facilities) that service the Public and Private sectors.
6. A means for identifying people world-wide in support of ***eVETTING*** that can be used to safeguard our borders and track aliens while in the country. Anyone wanting to enter the USA, for any reason, will have a Passport and VISA utilizing Bio-Metrics. The Bio-Metric Smart Card would be generated at the country of origin, with those records made available to support ***eVETTING*** through the individual granting access under secured conditions (think HIPPA and Identify Laws world-wide).
7. Secured borders and the ability to locate Aliens who have overstayed their allowed time within the country.

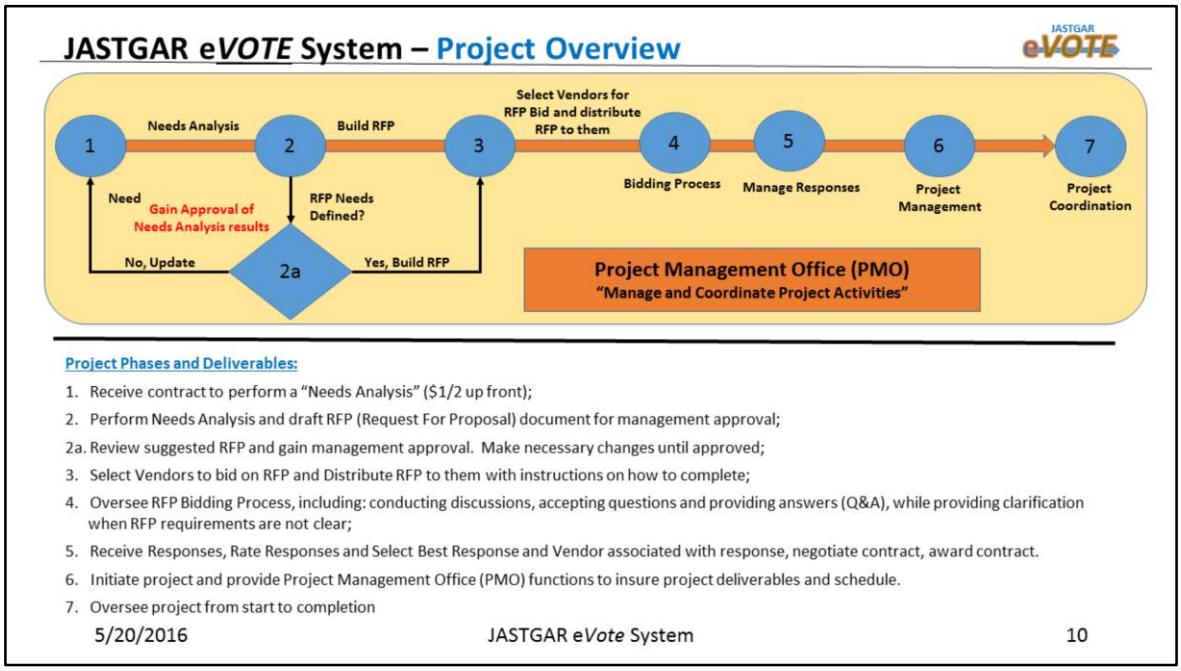


All voting locations associated with the Country's election process are tied together via the internet, using **secure environments** that incorporate:

1. Firewalls,
2. Access Controls,
3. Security Penetration Attempt Detectors
4. Vector Penetration Attempt Detectors
5. Security Information Event Management (SIEM) and Continuous Monitoring (CM) providing Alerts, Alarms, and Automated Activation of Responses
6. Encryption (Both for Data-At-Rest and Data-In-Motion) and
7. HTTPS security to support communications
8. Role Based Access Control (RBAC) technology for entitlements.

Additional **Security** will be added as new developments are announced, or as needed.

Combining Voter Bio-Metrics and Voter ID Card scans will identify voters who are authorized to vote and those that are in the process of committing a fraud (not the person identified on the card or they had previously voted in this election). Alerts will inform the Security Guard of the fraud being committed in real-time so they can identify, apprehend, detain, question, and perhaps prosecute violators with the audit trail and documentation provided by the system for support.



The **project phases** associated with implementing ***eVOTE*** are displayed above and include:

1. Needs Analysis
2. Engineering and Architectural Designs
3. Statement of Work
4. Project Plan
5. Schedule of Deliverables
6. Resource Usage and Costs
7. Systems Development Life Cycle
8. Disaster Recovery
9. Security and Auditing
10. Load Balancing and Error Handling
11. Alerts and Actions driven through system events and planned circumventions.
12. Support and Maintenance going forward.
13. Change and Release Management to resolve problems, implement enhancements, and add additional functions and features.
14. Best Practices for each of these disciplines will always be used.

JASTGAR e*VOTE* System – Project Details

Needs Analysis:
- Physical Investigation
- Location Analysis
- Infrastructure
- Population
- Voting Stations
- Voting Booths
- Voting Machines
- Network
- Security (Physical and Data)

Architectural Plan:
- Number of Locations
- Network
- Resources Requirements
- Infrastructure
- Utilities
- Personnel
- Voting Locations
- Local and International
- Special Considerations

Engineering Design:
- Design Specifications
- Resource Requirements
- Coding Parameters
- Inter-connections
- Resource Requirements Skills Matrix
- Product Needs
- Vendors who could help with products or services

RFP Process:
- RFP Creation
- Vendor Identification
- Vendors selected to receive RFP
- RFP Delivered to selected vendors
- Vendors complete RFP and return it to us
- We select vendors best qualified to help with products and services
- Team formulates and gets up to speed on exactly what we plan to do and how
- Everyone knows their part

SDLC:
- Development (*eCARD*, *eCARD APPs*, *eVETTING*, *eVOTE*, *eMEDICAL*)
- Testing
- Documentation
- Training
- Release Package
- Acceptance
- Transition
- Production Operations

Support, Maintain, Update, and Manage:
- Support Services will be provided
- Problem / Incident Management
- New Requirements and Enhancements
- Help Desk and Support Services procedures
- Problem Acceptance, Root Cause Analysis
- Mitigation Plans
- Mitigation Implementation
- Change Management
- Configuration Control Board
- Change Acceptance and Implementation
- Hot Fix or Change to be included in next Release
- Version and Release Management
- On-Going review of new Requirements, Features, and Enhancements to improve operation and efficiency

5/20/2016 JASTGAR e*Vote* System 11

- The "**Needs Analysis**" will perform a physical analysis of the locations to define the services and products needed to fulfill voting requirements for the population, including by voting stations, voting booths, Voting machines, and associated components.

- **Architectural and Engineering Plans** will be created to define the eVOTE environment, infrastructure, product, and service requirements, along with resource requirements from vendors and suppliers.

- An **RFP will be created** and sent to selected vendors that would define our needs and request proposals for assistance from the vendors.

- An **RFP Analysis and Vendor Selection** process will be accomplished.

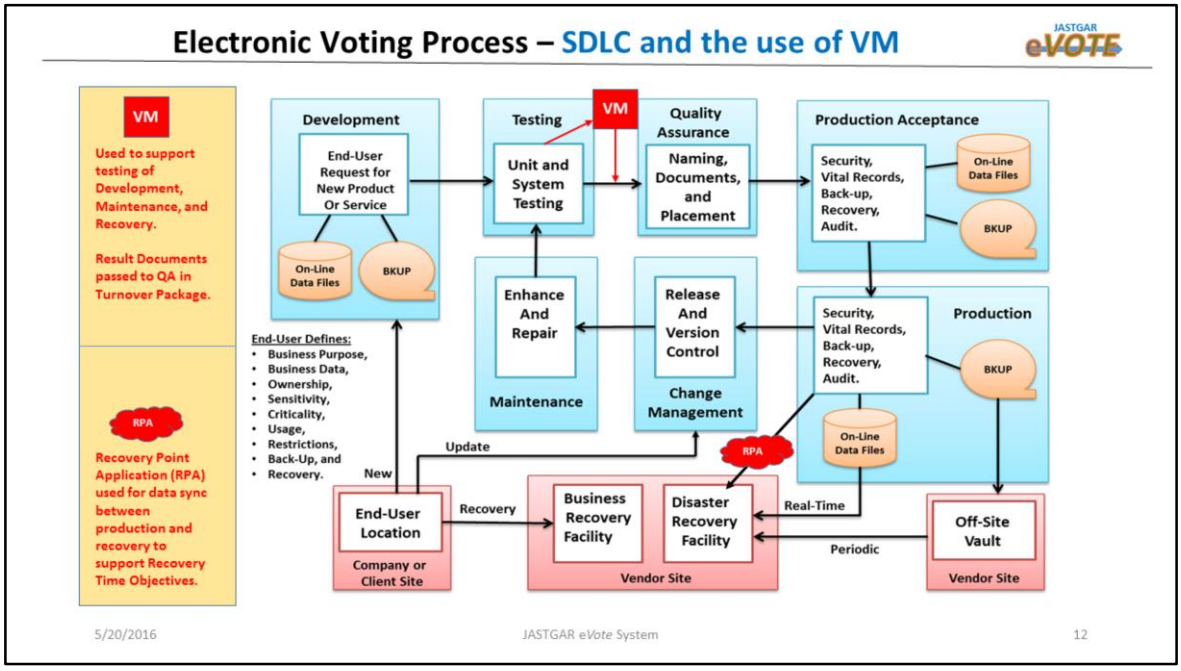
- A **Systems Development Life Cycle (SDLC**) will be defined based on "Best Practices" (see next slide).

- A **Production Ready Release Package** will be created that includes all application modules along with supportive documentation and training materials.

- An **Acceptance and Transition Process** will be created and adhered to when delivering JASTGAR products and services.

- **Support, Maintenance, and Version and Release Management** processes will be created and adhered to.

- **Change Management** guidelines will be created and followed whenever changes are needed to mitigate problems / incidents, implement enhancements, new requirements, and new features or vendor releases.



The SDLC environment is depicted above with the inclusion of VM (Virtual Machine) used to enhance testing and recovery operations. The process includes:

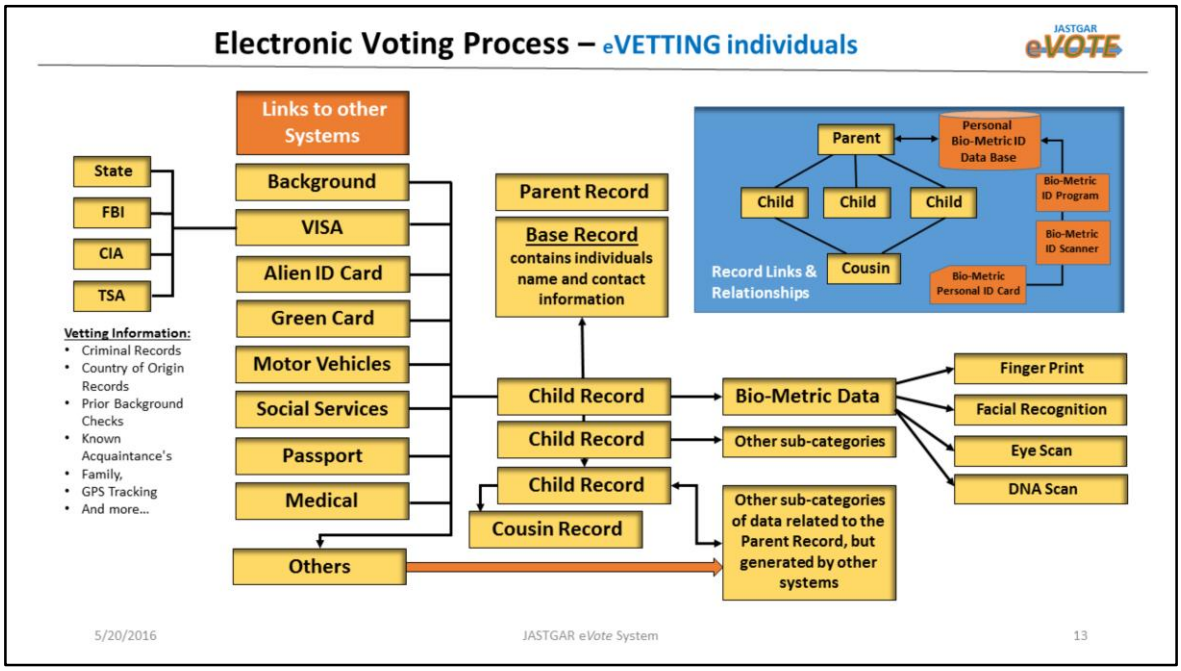
- **Develop** applications or services within the Development Environment (VM Machines used for Sandbox, Development, Testing, Acceptance, and Transition to Production Operations)

- **Testing** is performed within the VM environment that initially duplicates the Production Environment to validate that the newly develop application or service can successfully process within Production Operations. A second VM environment represents the disaster recovery environment and will support recovery testing prior to transitioning to production operations.

- **Off-Site vaulting** will be accomplished as needed.

- **Recovery Operations** will be supported through Business and System Recovery sites.

- **Data Recovery** will be supported by real-time, or near real-time, data backups between the production and recovery environments so immediate switchover can be accomplished if needed.

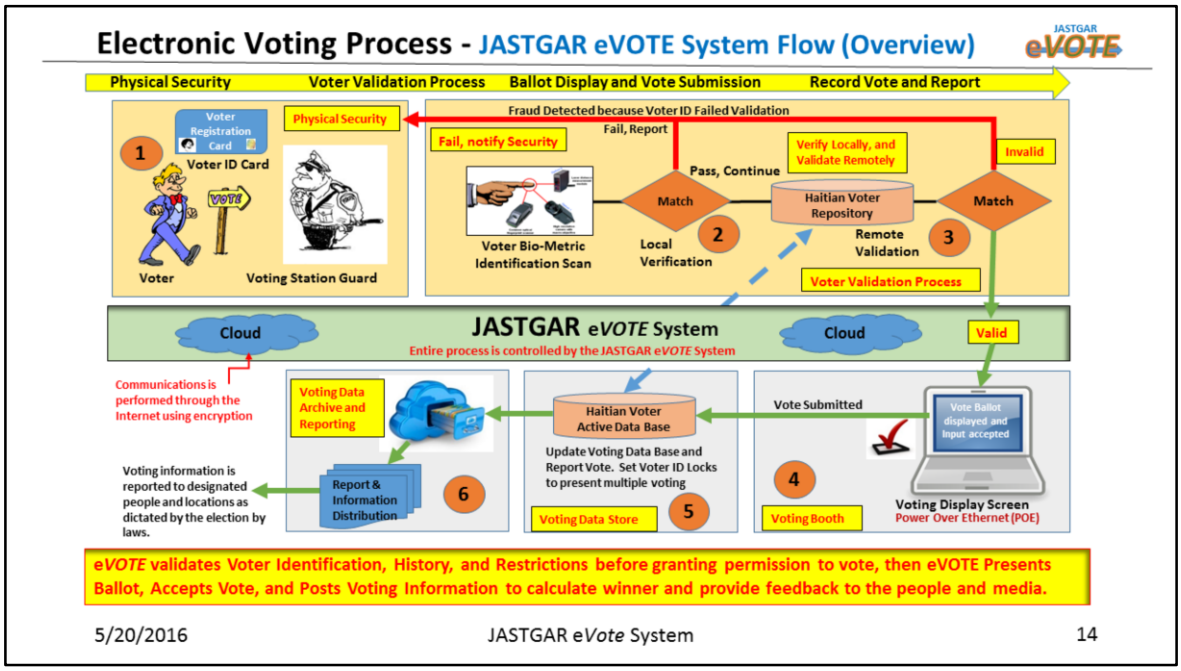


The **process of Vetting** individuals is shown within this slide as a data base record structure of Parent, Child, Cousin. The Parent record contains an individuals personal information, while Child records can contain public information that can be legally viewed as necessary. Cousin records can also be known as Associate records because they can be related to the people a Parent or Child record is associated with (like a member of a crime cell, or terrorist organization, etc.).

Comparing information contained within a Bio-Metric Smart Card with the Individual ID data base will validate that a person is who they claim to be.

The individual bio-metric information stored on our Smart ID Card can be used to **satisfy a range of needs**, from vetting individuals entering the country, through aiding the law enforcement industry, and health care industry. There is a simple process associated with activating and utilizing our systems, which includes the creation of a Bio-Metric Smart ID Card (***eCARD***) to how the card can be scanned and utilized. ***One card with many applications*** that can be accessed via ***eCARD APPs***.

The *eVOTE* electronic voting system is an example of combining *eVETTING*, *eCARD*, and *eCARD APPS* into a cohesive and complete service based on applications driven by *eCARD* users.

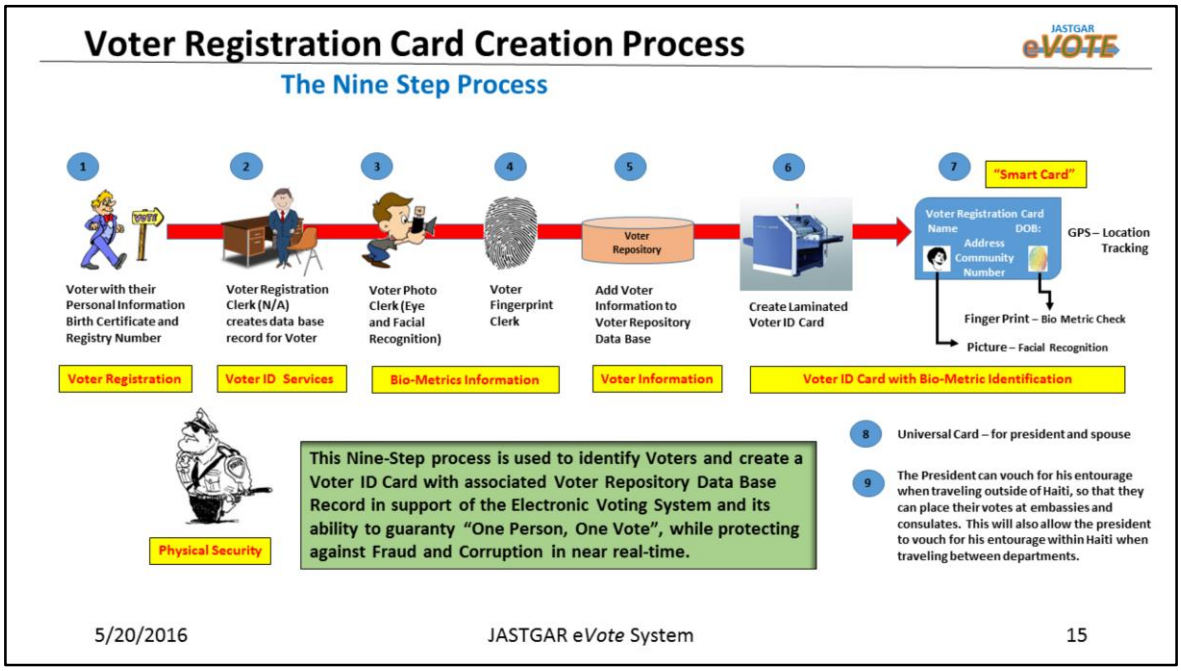


The **Voting Process** is depicted above. It includes physical security at Voting Stations to examine and validate voter identity locally and a remote data base scan of the voter's voting record to detect attempts to double-vote or if they actually allowed to vote.

Should a **fraud** be committed, either because the Voter ID card does not match the Voter, or the Voter has already voted in the election, then Physical Security will be immediately notified and the offender immediately taken into custody for questioning and possible prosecution.

Our system is designed to **eliminate voter fraud and corruption** by taking immediate action, while an audit trail and documentation produced by the system are used to prosecute criminal acts. Collected Security documentation includes:

1. Voter Bio-Metric comparisons (Eyes, Face, Finger Prints, etc.)
2. Voter snapshot when they place their vote
3. Audit trail of voter activity stored in our data base.
4. Voting displays and reports that can be sent to authorized personnel
5. Near real-time voting results



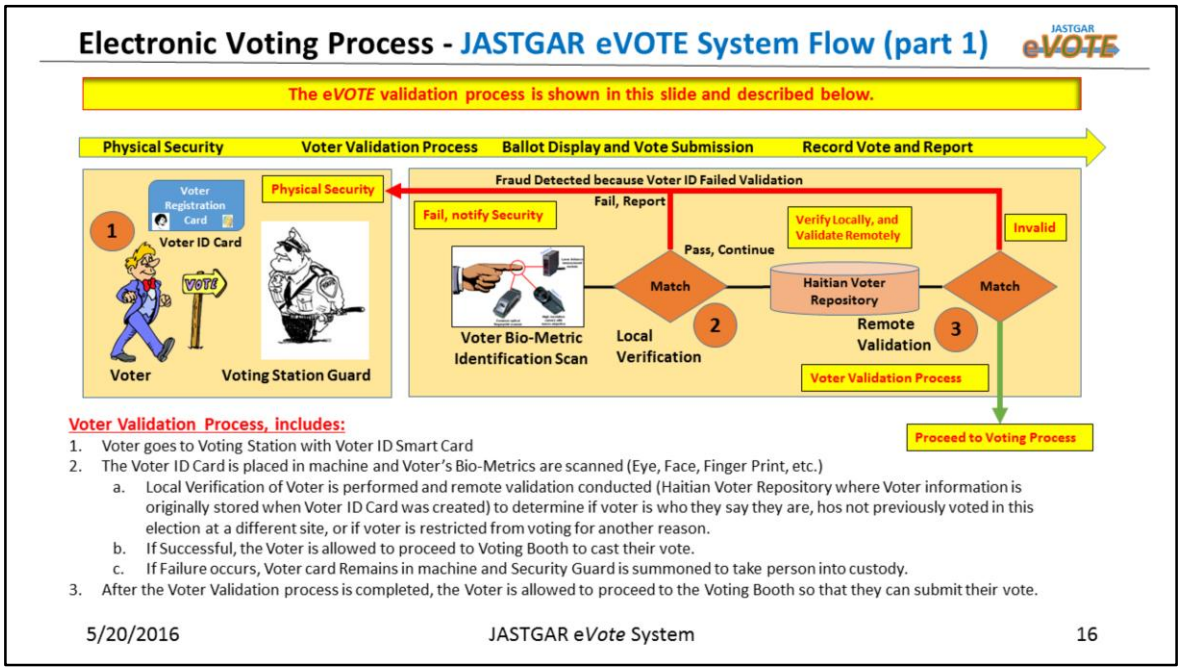
The **Voter Registration** process is shown above. It includes collecting and validating voter identity and contact information and producing a Voter ID Record containing Bio-Metric information that validates a voter's identity. This information is added to our data base and included in the Voter ID Card we produce.

The **Voter ID Card verifies** the voter is who they say they are, while the data base information tracks their voting record and is used to eliminate double voting.

Utilizing "**Smart Card**" technology will allow us to lock the Voter ID Card in the scanning machine until the voter's identity and voting record are validated. If successful the card is returned to the voter, but if unsuccessful the card is retained and the person committing the fraud is detained and possibly arrested.

System records, including pictures of when the voter actually voted, will be provided to prosecutors as needed to convict people attempting to commit a fraud or corrupt act.

As word of this system's security becomes public, fewer people will even attempt to commit frauds or practice corruption.



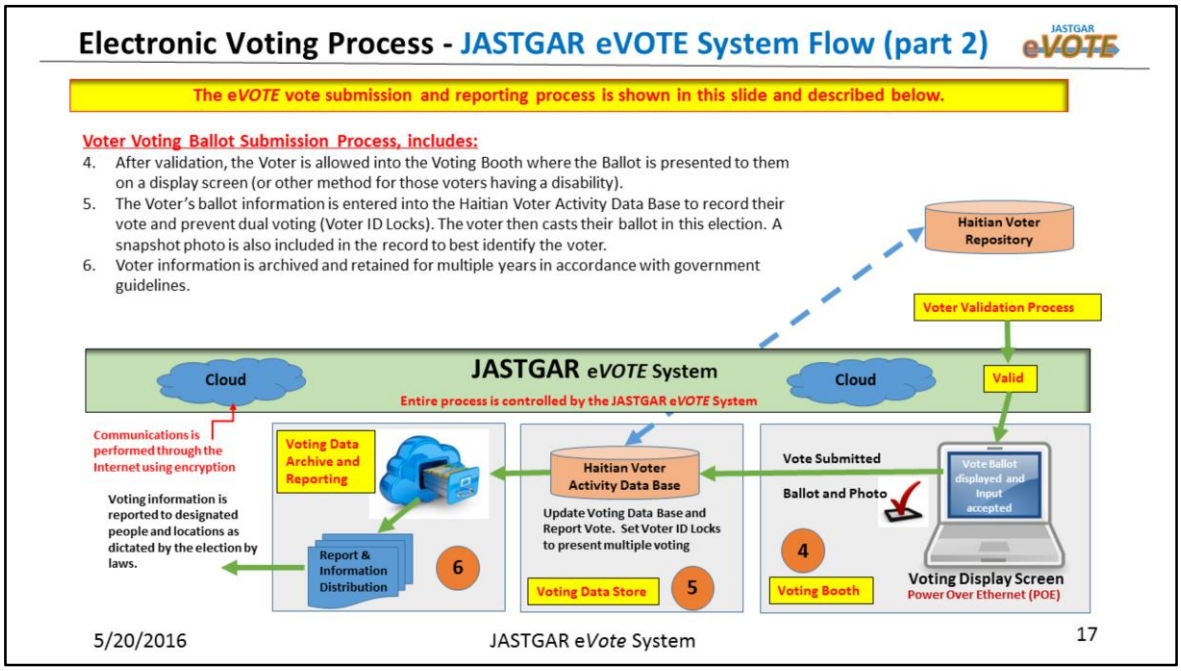
The **initial process** conducted by the ***eVOTE*** system is to validate that the Voter is who they claim to be and that they are allowed to cast a ballot at this Voting Station. This is accomplished in a three step process, which is:

1. **Locally verify** that the Voter is who they claim to be by having the Voter insert their Voter ID Smart Card into a Bio-Metric Scanner, which scans the Voter's Bio-Metric Signature (Eyes, Face, Finger Prints, etc.) and compares it against their Voter ID Card.

2. **Remotely Validate** the Voter by comparing their Bio-Metric information to the Country's Voter Repository (where their original Voter ID information was stored when they received their Voter ID Card). After validation, the Voter's record is scanned to determine if they have previously voted in this election, or if they have restrictions against being allowed to vote. We also check the Eligible Voter List.

3. **If successful**, the Voter is allowed to cast their ballot in this election.

When the Voter has been successfully validated, they are allowed to "**Proceed to Voting Process**" where they are presented with a Ballot and allowed to Cast Their Vote.



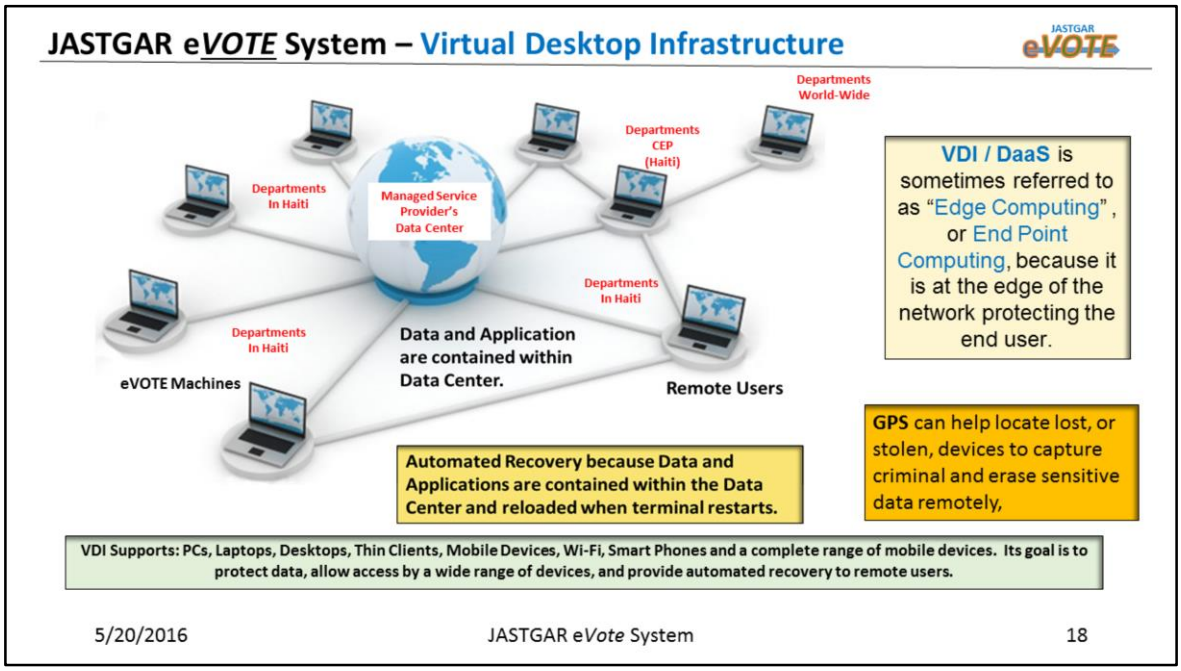
Once a Voter has been Validated, they are allowed to proceed to the Voting Process, where the following steps are taken.

4. The Voter **enters the Voting Booth** and inserts their Voter ID Card. A Ballot is presented to them via a Display Screen (Voter's with disabilities will have special procedures for providing them with appropriate Ballots). Help information is provided with the Ballot information along with a Language Selection option.

5. The **Voter submits their vote** by completing the Ballot. Once completed, the voter extracts their Voter ID Card and proceeds to the Voting Station Exit. The Voter's Ballot information is transferred to the Country's Voter Activity Data Base for Tallying and display via the media.

6. The Country **Voter Activity Data Base is archived** for the period of time designated by government regulations. From this information, trending analysis is performed and an Audit Trail preserved to support voter fraud and corruption charges going forward.

The ***eVOTE*** system is designed to support the voting process through the use of current technology, so that "***One Person – One Vote***" can be supported and to capture, document, and prosecute anyone committing Voter Fraud or Corruption. We hope you agree with our direction and philosophy.

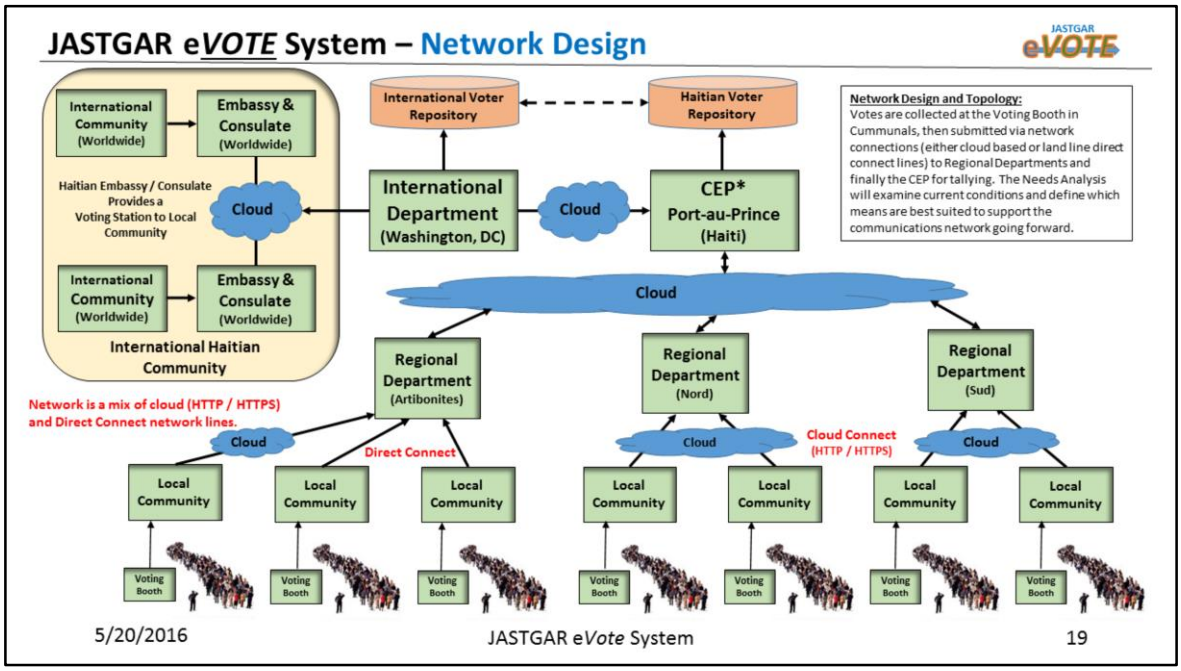


Utilizing **Virtual Desktop Infrastructure** (VDI) will protect the Voting System and reduce costs dramatically by using terminals that are stripped down to their base essentials (no external drives).

The **voting programs and data are maintained remotely** at the data center, so if a terminal should fail the voter can move to a working terminal and pick up where they left off without any loss of data. These devices do not have any external storage devices connected to them so nobody can place a USB drive or CD into the machine to load votes into the system

The **terminals used within a VDI system** are much cheaper than normal PC's because they have fewer parts. Maintenance is easier and less costly because changes made at the data center are automatically made available to all VDI terminals, which will guaranty that the system is maintained in a current state at all times.

If a **VDI terminal is stolen**, or lost, it can be tracked via GPS and any information contained in a VDI device can be remotely erased. Therefore, using VDI can result in capturing people who attempt to steal the equipment, while insuring that data is not accessed, lost, or corrupted.



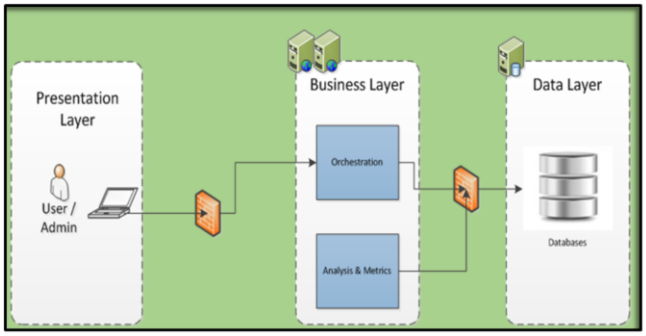
All locations associated with the Country voting system will be connected through the Internet, even remote voting locations at embassy's and consulate's.

Cloud communications technologies that incorporate security controls and encryption will be used to communicate between remote voting stations and the ***eVOTE*** system.

All information will be encrypted during transport and when stored (end-to-end encryption), so data integrity can be maintained at all times and data cannot be intercepted and changed by someone trying to commit fraud or corruption.

The **data base system is archived** at the end of the election, so that history and trending analysis can be conducted.

JASTGAR e*VOTE* System – Security Layers



Security is embedded within the application between the Network and the Application, which provides:

- User to application ***Security*** via Firewall and Application Access ***Controls*** using Application ID, User ID and Password
- ***Application to Data Bases*** via Firewall and Access Controls
- ***End-to-End Encryption***

Key points to note about the N-Tier approach include the following:

- Systems and services are ***logically separated*** to isolate business functions
- Each ***tier communicates*** only with the adjacent tier
- ***Specific security*** services are provided within each tier to ensure defense in depth across the entire deployment

These fundamental ***safeguards and countermeasures*** are recommended to protect information during processing, while in storage and during transmission. The specific configuration of the organization network topology, however, will likely require additional considerations not described here.

The JASTGAR e*VOTE* Information Security Policy defines the fundamental principles for the protection of Company information resources, the controls needed to best ensure compliance with internal and external regulations, and to uphold the JASTGAR reputation of excellence with its clients. All personnel are responsible for ensuring compliance with JASTGAR e*VOTE* Information Security Policy.

Role Based Access Control (RBAC) is used to define user entitlements and support security coding for individual access to data and physical locations. ***eCARD*** can be used to govern user security access rights either as an access card for doorways or computers.

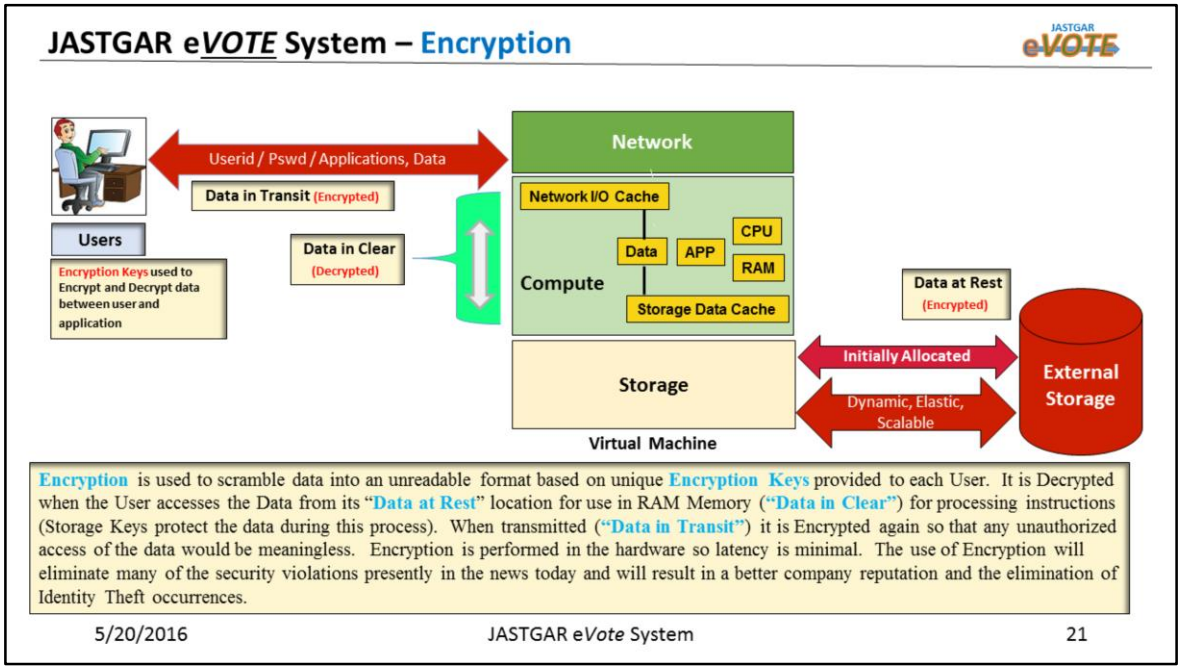
5/20/2016 JASTGAR e*Vote* System 20

End-to-End security features incorporated in the **e*VOTE*** system are described above.

The **JASTGAR e*VOTE*** system ensures **only authenticated users have access** to the system and all authenticated users are **further restricted based on** the authorization roles, groups and individual data records assigned to the authenticated users (Role Based Access Control – RBAC).

Additionally the JASTGAR e*VOTE* system will **operate a behind the boundary security system** of the hosting organization infrastructure (i.e., on the hosting Local Area Network (LAN/Intranet). To ensure data and system confidentiality, integrity, availability and non-repudiation. The JASTGAR e*VOTE* system relies on a network architecture that provides a **layered defense** (hardened systems, network separation, auditing, login rights and intrusion prevention/detection) against internal and external network threats.

The above figure illustrates a general layout of this type of structure at a very high level

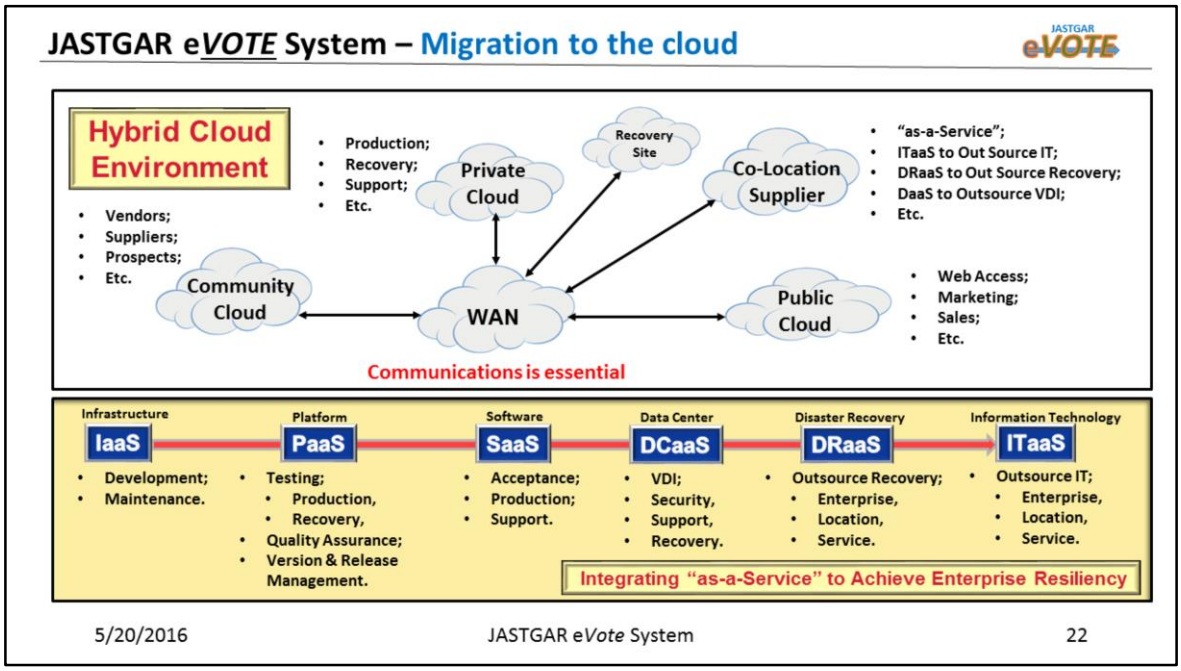


How encryption is used within the eVOTE system is demonstrated above.

Both "**Data-at-Rest**" and "**Data-in-Motion**" are encrypted, while data being processed by the program is decrypted under the hood of the computer where memory security rules prevent data intrusion.

The only time that data is in the clear (not encrypted) is when it is being processed by a program. System safeguards will protect the data while it is being processed. Our encryption of data while it is stored or transported will insure the integrity of the data from end-to-end.

Network security will include Firewalls, Security Information Event Management (SIEM), Intrusion Detection, and Persistent Threat investigation tools. Vulnerability of hardware and software will be continuously monitored and improvements made to the configuration in the form of configurations, elimination of vulnerabilities via patches, alert generated when thresholds are crossed, action items for repairs, enhancements, and all other methods used to safeguard an environment.



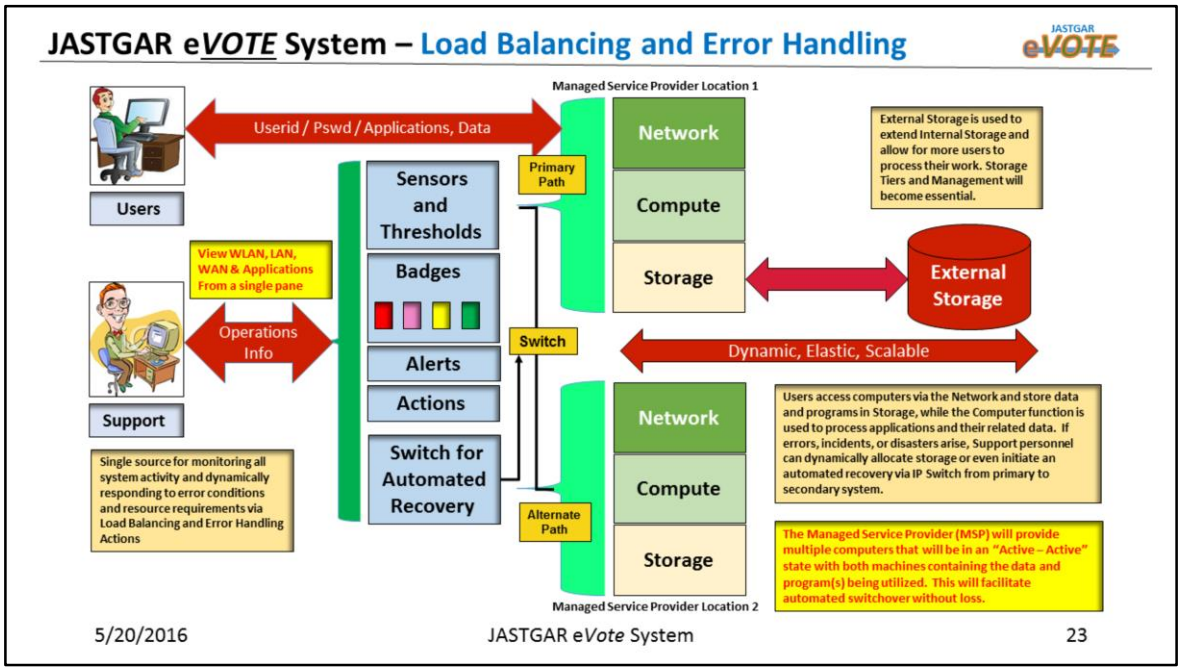
Migrating the eVOTE system to the cloud environment will provide a much higher level of security, while allowing for the dynamic control of resources to best respond to voting demands.

Utilizing a Managed Service Provider (MSP) for this purpose would greatly reduce costs and provide for a much higher level of security through disaster recovery and load balancing.

Communicating via the Internet and a Wide-Area-Network (WAN) will speed operations and provide an enhanced level of security.

Utilizing the latest technologies for controlling the Storage, Transportation, and Computing of information will result in the development of a Software Defined Data Center (SDDC) that compliments the Software Defined Network (SDN) and Software Defined Storage (SDS) environments.

Incorporating a Recovery Site within the system architecture will allow for immediate switchover from a failing system to an operating system.



The **cloud environment** will allow for Load Balancing and Error Handling by the following methods:

1. **Badges** are used to illustrate operation (i.e., Green is good, Yellow is degrading, and Red is bad),
2. **Sensors** are used to monitor thresholds and when the system moves across a threshold the badges are used to generate an alert,
3. **Alerts** send messages and warnings to appropriate personnel (emails, text messages, etc.),
4. **Actions** are instructions provided to personnel related to an alert, or they can be canned activities that are automatically executed in response to an alert (i.e., machine is broken, switch to secondary unit and reconnect to that unit, send error report to technical staff to replace / repair failing unit),
5. **Software Defined Data Centers** (SDDC), Networks (SDN), and Storage (SDS) all work together to respond to resource needs and maintain an optimized processing environment,
6. **You only pay for what you use** in a Managed Service Environment and you can regulate your costs within a Service Level Contract.
7. **The Managed Service Provider's system** will increase of decrease services to match your desired bill as defined in your Service Level Contract.
8. **Managed Service Provider personnel** can assist in creating, monitoring, and responding to problems in your system

Electronic Voting System development activities

Where do we go from here

1. Contract with JASTGAR to serve as the Project Contractor, responsible for coordinating the construction and delivery of this Electronic Voting System, and including the selection and hiring of subcontractors to fulfill specific work items needed to complete the system and requiring special skills and talents.
2. Contract JASTGAR to perform the Needs Analysis Phase, with ½ of the funding requirements provided up-front to support JASTGAR activities. JASTGAR incurred expenses for Living and Travel will be paid for by the Government.
3. Guaranty to JASTGAR that the program product being constructed will be solely owned by JASTGAR, who is the designer of the system and patent holder.
4. Agreement to work with Country's Government to sell product to other countries that may want to follow in the path set forth by this project, with an agreed upon commission fee to be paid to the Government for their assistance in obtaining the new business for JASTGAR.
5. On-Going contract for JASTGAR to provide Support and Maintenance for the Electronic Voting System.

5/20/2016 JASTGAR e*Vote* System 24

JASTGAR would like to maintain the position of Contractor throughout this project, hiring appropriate sub-contractors as needs arise. Our approach is described above and the deliverables you can receive include:

1. ***eCARD*** to identify people based on their bio-metric signature.

2. ***eVETTING*** to guaranty people are who they say they are and to insure only. authorized people can use the application / service or can gain approval to enter locations.

3. ***eCARD APPS*** to support applications and services based on an individual's identity being guaranteed.

4. ***eVOTE*** to conduct electronic elections and improve voter services.

5. ***eMEDICAL*** to provide citizens with a higher level of healthcare services via DNA analysis and treatment guidelines (Allergic to Drug, Dosage Recommendations, etc.)

Electronic Voting Process – What's in it for you

1. Fully implemented "Electronic Voting System" based on your specific needs.
2. "One Person – One Vote", guaranteed.
3. Establishment of a "Voter Recognition System", complete with:
   - Voter identification cards,
   - Bio-Metric data stored in *eCARD* Chip to support local identification,
   - Remote determination of an individual's rights and authorizations,
   - Electronic Voting system at voting stations to validate voters and collect votes,
   - Vote reporting and display system for rapid vote response and publication,
   - Well documented and supported electronic voting system,
   - Trained voting staff, government officials, and voters, and
   - Support and maintenance services going forward.
4. Best Practices used to design, build, test, and implement the system that is above political liabilities.
5. Well trained voter population who knows how to use the system and approves of its operation.
6. Electronic Vote collection both locally in Haiti and internationally in embassies and consulates.
7. Worry-free operation and support of the electronic voting system, so that political representatives will not be associated with corruption or voter fraud.
8. A safe and secure election that is a true representation of the people's voting desires.

5/20/2016 JASTGAR e*Vote* System 25

The benefits that you will receive through this effort are described within this slide. We hope you believe in the JASTGAR approach and the benefits you will receive and that you want to hire JASTGAR as the project contractor to implement the electronic voting system best suited to meet your needs.

JASTGAR e*VOTE* System – Appendix 'A" - Real ID Act (part 1)

Minimum Document Requirements:

1. The person's full legal name.
2. The person's date of birth.
3. The person's gender.
4. The person's driver's license or identification card number.
5. A digital photograph of the person.
6. The person's address of principle residence.
7. The person's signature.
8. Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes.
9. A common machine-readable technology, with defined minimum data elements.

Minimum Issuance Standards:

1. **IN GENERAL-** To meet the requirements of this section, a State shall require, at a minimum, presentation and verification of the following information before issuing a driver's license or identification card to a person:
   a. A photo identity document, except that a non-photo identity document is acceptable if it includes both the person's full legal name and date of birth.
   b. Documentation showing the person's date of birth.
   c. Proof of the person's social security account number or verification that the person is not eligible for a social security account number.
   d. Documentation showing the person's name and address of principal residence.

SPECIAL REQUIREMENTS:

A. **IN GENERAL-** To meet the requirements of this section, a State shall comply with the minimum standards of this paragraph.

A. **EVIDENCE OF LAWFUL STATUS** - A State shall require, before issuing a driver's license or identification card to a person, valid documentary evidence that the person –
   I. is a citizen or national of the United States;
   II. is an alien lawfully admitted for permanent or temporary residence in the United States;
   III. has conditional permanent resident status in the United States;
   IV. has an approved application for asylum in the United States or has entered into the United States in refugee status;
   V. has a valid, unexpired nonimmigrant visa or nonimmigrant visa status for entry into the United States;
   VI. has a pending application for asylum in the United States;
   VII. has a pending or approved application for temporary protected status in the United States;
   VIII. has approved deferred action status; or
   IX. has a pending application for adjustment of status to that of an alien lawfully admitted for permanent residence in the United States or conditional permanent resident status in the United States.

5/20/2016 JASTGAR e*Vote* System 26

The Real ID Act was passed by both the House of Representatives and the Senate in response to concerns raised after 9/11 and recommendation made by the 9/11 Review Commission. Its purpose is to validate that a person is who they claim to be.

The next three slides provide pertinent information from the actual text of the Real ID Act H.R. 1268.

In all cases eCARD meets, or exceeds, the requirements contained within the Real ID Act.

Minimum Document Requirements pertain to a persons Name, DOB, Gender, Driver's License number, a Digital Photo (for Facial Recognition), permanent address, signature, and the card must have physical security features to protect against fraudulent duplication, all meeting machine readable technology standards.

Minimum Issuance Standards include proof of SS#, proof of DOB, an acceptable Photo ID.

Special Requirements applies to immigrants and aliens on VISA.

JASTGAR e*VOTE* System – Appendix 'A" - Real ID Act (part 2)

VERIFICATION OF DOCUMENTS –

To meet the requirements of this section, a State shall implement the following procedures:

(A) Before issuing a driver's license or identification card to a person, the State shall verify, with the issuing agency, the issuance, validity, and completeness of each document required to be presented by the person under paragraph (1) or (2).

(B) The State shall not accept any foreign document, other than an official passport, to satisfy a requirement of paragraph (1) or (2).

(C) Not later than September 11, 2005, the State shall enter into a memorandum of understanding with the Secretary of Homeland Security to routinely utilize the automated system known as Systematic Alien Verification for Entitlements, as provided for by section 404 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (110 Stat. 3009-664), to verify the legal presence status of a person, other than a United States citizen, applying for a driver's license or identification card.

eCARD meets, or exceeds, all of the Real ID Act requirements

Other Requirements –

To meet the requirements of this section, a State shall adopt the following practices in the issuance of drivers' licenses and identification cards:

(1) Employ technology to capture digital images of identity source documents so that the images can be retained in electronic storage in a transferable format.
(2) Retain paper copies of source documents for a minimum of 7 years or images of source documents presented for a minimum of 10 years.
(3) Subject each person applying for a driver's license or identification card to mandatory facial image capture.
(4) Establish an effective procedure to confirm or verify a renewing applicant's information.
(5) Confirm with the Social Security Administration a social security account number presented by a person using the full social security account number. In the event that a social security account number is already registered to or associated with another person to which any State has issued a driver's license or identification card, the State shall resolve the discrepancy and take appropriate action.
(6) Refuse to issue a driver's license or identification card to a person holding a driver's license issued by another State without confirmation that the person is terminating or has terminated the driver's license.
(7) Ensure the physical security of locations where drivers' licenses and identification cards are produced and the security of document materials and papers from which drivers' licenses and identification cards are produced.
(8) Subject all persons authorized to manufacture or produce drivers' licenses and identification cards to appropriate security clearance requirements.
(9) Establish fraudulent document recognition training programs for appropriate employees engaged in the issuance of drivers' licenses and identification cards.
(10) Limit the period of validity of all driver's licenses and identification cards that are not temporary to a period that does not exceed 8 years.
(11) In any case in which the State issues a driver's license or identification card that does not satisfy the requirements of this section, ensure that such license or identification card–
  a. clearly states on its face that it may not be accepted by any Federal agency for federal identification or any other official purpose; and
  b. uses a unique design or color indicator to alert Federal agency and other law enforcement personnel that it may not be accepted for any such purpose.
(12) Provide electronic access to all other States to information contained in the motor vehicle database of the State.
(13) Maintain a State motor vehicle database that contains, at a minimum–
  a. all data fields printed on drivers' licenses and identification cards issued by the State; and
  b. uses a unique design or color indicator to alert Federal agency and other law enforcement personnel that it may not be accepted for any such purpose.

(12) Provide electronic access to all other States to information contained in the motor vehicle database of the State. (13) Maintain a State motor vehicle database that contains, at a minimum–
  a. all data fields printed on drivers' licenses and identification cards issued by the State; and
  b. motor vehicle drivers' histories, including motor vehicle violations, suspensions, and points on licenses.

5/20/2016 JASTGAR e*Vote* System 27

States must implement:

Verification of Documentation prior to issuance of any document

Other Requirements pertains to:

technology, retention, facial geometry, confirmed SS#, insuring that people having identification from another state have terminated that state's identification prior to issuing identification ID in this state, ensuring the physical security at issuing agencies protect against theft of blank documents and cards, ensure all issuing personnel have proper security clearance, establish fraudulent documentation capturing techniques, assign a validity period to all issued documents to insure renewal and re-verification, if state does not meet minimum requirements for Real ID then that must be clearly stated on issued document, provide electronic access to other states, maintain a state motor vehicle data base including all the information contained on an issued document, and motor vehicle history records.

JASTGAR e*VOTE* System – Appendix 'A" - Real ID Act (part 3)

SEC. 203. TRAFFICKING IN AUTHENTICATION FEATURES FOR USE IN FALSE IDENTIFICATION DOCUMENTS.

A. Criminal Penalty- Section 1028(a)(8) of title 18, United States Code, is amended by striking `false authentication features' and inserting `false or actual authentication features'.

B. Use of False Driver's License at Airports-

1. **IN GENERAL -** The Secretary shall enter, into the appropriate aviation security screening database, appropriate information regarding any person convicted of using a false driver's license at an airport (as such term is defined in section 40102 of title 49, United States Code).
2. **FALSE DEFINED -** In this subsection, the term `false' has the same meaning such term has under section 1028(d) of title 18, United States Code.

SEC. 204. GRANTS TO STATES.

(a) In General - The Secretary may make grants to a State to assist the State in conforming to the minimum standards set forth in this title.

(b) Authorization of Appropriations - There are authorized to be appropriated to the Secretary for each of the fiscal years 2005 through 2009 such sums as may be necessary to carry out this title.

SEC. 205. AUTHORITY.

(a) Participation of Secretary of Transportation and States - All authority to issue regulations, set standards, and issue grants under this title shall be carried out by the Secretary, in consultation with the Secretary of Transportation and the States.

(b) Extensions of Deadlines - The Secretary may grant to a State an extension of time to meet the requirements of section 202(a)(1) if the State provides adequate justification for noncompliance.

These sections outline the laws pertaining to violation of the Real ID Act, States Power, and Authority to pursue this act.

Electronic Voting Process – Acronym Table

ACRONYM Table	
RFP	Request For Proposal
PMO	Project Management Office
POE	Power Over Ethernet
VIC	Voter Identification Card
VBM	Voter Bio-Metric
HVR	Haitian Voter Repository
VDI	Virtual Desktop Infrastructure
CPE	Counsel Electoral Provisory
PERS	Personal Client
GOV	Government Client
BUSI	Business Client

The acronym's used in the JASTGAR eVOTE system are explained above. This table will be maintained as new acronyms are created.

Any questions, comments, or recommendations can be sent to Tom Bronack or Alex Jecrois at:

Alex Jecrois	ajecrois@Hotmail.com
Tom Bronack	bronackt@gmail.com

We would love to discuss how our products can help you achieve your goals of insuring a person's identity prior to providing them access to you location, services, or applications.0