FVAP.GOV — *Voting Help For Uniformed Service Members, Their Families, & Citizens Living Outside the United States*

Texas Effective Absentee Systems for Elections (EASE) Grant

FULLY Funded by the Federal Voting Assistance Program (DoD)

Frequently Asked Questions (FAQ)

"Your Texas – Your Vote"

Rockwall County and 49 Texas counties, partnered with Democracy Live

Index

"Your Texas – Your Vote" Grant Application

The goal of the grant application to the Federal Voting Assistance Program is to provide every military & overseas voter with the opportunity to receive their ballots with greater ease. The biggest problem regarding our military & overseas voters is the time it takes for them to receive their ballots, vote and returned their voted ballots back to the Elections office.

Rockwall County leads the *Your Texas – Your Vote,* which is the largest consortium of grant applicants in the United States to be awarded funding by FVAP.

Why should Texas Counties join this consortium?

- Compliance with the Federal MOVE Act which states that states must meet the 45 day round trip for each ballot to be returned by regular mail.
- LiveBallot provides a web-based on demand ballot delivery system that provides our military & overseas voters faster access to their ballots.
- LiveBallot is CURRENTLY the most widely used Sample Ballot partner in Texas.
- As a whole, the consortium shows the Federal Voting Assistance Program that Texas and counties in particular are serious about our Military & Overseas voters getting their chance to vote.

The grant will help the consortium of counties to use this grant to meet the goal of the grant and the MOVE Act.

This presentation addresses the FAQ about the "Your Texas – Your Vote" Consortium.

Question #1 – Political Party Support

Does this project have bi-partisan support?

Answer – Yes.

Both Republican and Democratic Parties support efforts to make the voting process easier for Military and Overseas Voters. These are sample responses provided by Rockwall County:

"As Chairman of the Rockwall County Republican Party, I support this initiative. It appears to me there are additional manual procedures that can be removed; however, this is a step in the right direction. Happy to support this…."

Tony Fisk
Chairman
Rockwall County Republican Party

"After reading more about the current voting process for the military I am in favor of applying for the grant which enables our military and overseas voters to receive a ballot on line.

I also spoke with a number of my Executive Committee who are also in favor of applying for the grant.
.
Thanks for the work you have done on this,"

Judith Matherne, County Chair
Rockwall Democratic Party

"We currently use an email program & to me, it makes it harder for the military & overseas voter to receive his ballot because he has to download attachments. In the new program, he does not.

Using our current system, many times, we received calls & emails from voters saying they cannot download the attachments, especially aboard ships. The new program, the voters just prints the documents because they are part of the program.

Also, there is no tracking system with the old plan. Neither the elections office or the voter can track the application or ballot. The new plan not only has a tracking plan, it will email the voter & let him know if his application is received, when the ballot was mailed out, when it was received back & will also let the voter know at the end of the year that his application is about to expire & to send a new one.

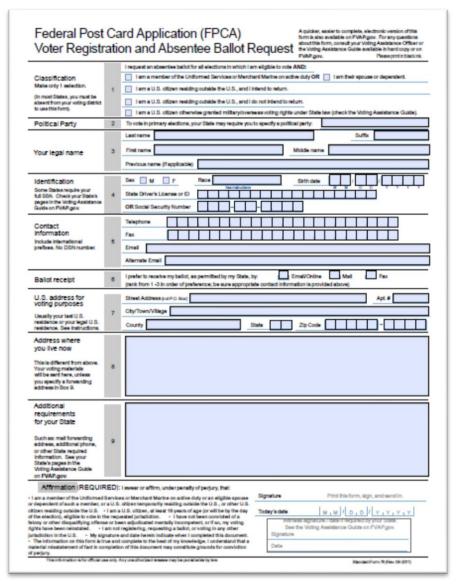*In my opinion, the new system provides better access, function & security for the voters."*

Glenda Denton, CERA (Certified Elections/Registration Administrator)
Elections Administrator

Question #2 (Federal Post Card Application)

The military and overseas voters do not have access to computers and printers, so why are we sending their ballots to them by email?

Answer

All military and overseas voters prepare a Federal Post Card Application (FPCA). On line #6, the voter indicates how they would like their ballot sent to them. WE must honor their preference. A copy of the FPCA is below:
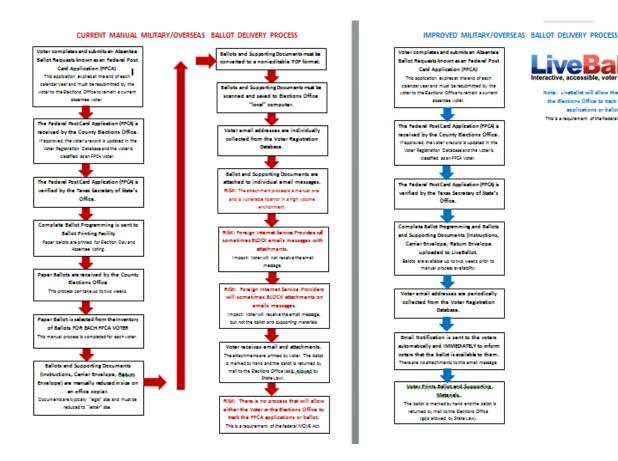
Question #3 (Workflow Illustrations)

What is the current process in the Elections Office for handling the military and overseas ballots and how will the new system make it easier for the voters to receive their ballots?

Answer

A flow chart is being included which show the current process and how the new improved process will work. (Full size documents on following pages):

Question #4 (Security)

What about security issues and how can we be sure that the voter's ballot is protected?

Answer

The "Your Texas – Your Vote" Consortium of Counties and Democracy Live are committed to making sure that the voter's ballot is received in a secure method. A description of the security measures to protect the ballot are detailed here:

LiveBallot - Strong Security

Secure system hosting and data protection

Voter information and election data uploaded to LiveBallot are safely stored on the Microsoft Secure eGovernment Cloud Platform and is protected by 228-bit access and view applications and data running on the secure servers.

Voter privacy

Leveraging Microsoft's Azure, the second largest secure hosting environment in the U.S., second only to the U.S. Department of Defense (DoD), LiveBallot balloting and voter data are protected with the assurance of the largest software and security company in the world.

The secure hosting environment securely stores voter registration data (e.g. Name, Address, Party Affiliation, Precinct, etc.) to permit voter lookup and matching to the appropriate ballot style.   To protect voter privacy, the LiveBallot platform applies security mechanisms at different layers of the cloud infrastructure to implement a defense-in-depth approach. These layered mechanisms include:

- Physical security of the data centers (locks, cameras, biometric devices, card readers, alarms);
- Firewalls, application gateways and IDS to protect the network;
- Access Control Lists (ACLs) applied to virtual local area networks (VLANs) and applications;
- Authentication and authorization of persons or processes that request access to data;
- Hardening of the servers and operating system instances;
- Redundant internal and external DNS infrastructure with restricted write access;
- Securing of virtual machine objects; and

- Securing of static and dynamic storage containers.

Assets are categorized as to the level of security required, based on the potential for damage. Highly sensitive assets are protected by more stringent mechanisms, such as multi-factor authentication (smart cards, biometrics, and hardware tokens). The principle of least privilege is followed, whereby persons and processes are given the lowest level of access that is required for them to do their jobs and no more.

LiveBallot is deployed within Microsoft Global Foundation Services datacenters, and thus enjoys the world-class network security and privacy benefits provided by Microsoft's robust, industry leading security protocols.

Strong passwords

LiveBallot password requirements are able to use strong password requirements that include an eight character or more passwords that contains alpha, numeric, and symbol characters

The LiveBallot solution protects the voter's privacy, as well as the election data, with its combined front and back end proven scalable secured hosting environment. LiveBallot's proven and highly scalable hosting environment protects voter data on the front end using secure SSL encryption, automatically expiring a voter's session on the website, and limiting the information stored in the voter's session.

Scalability, security and stability are the key reasons LiveBallot is hosted in the Microsoft Azure cloud environment. With a proven and sustained uptime on a 24x7 basis, and real time, multi-geographic server redundancy, the system will render the ballots as required.

Our commitment to security makes the Live Ballot system a highly reliable system with no known loss of ballot delivery occurrences over prior deployments. Redundancy in the architecture also provides the ability to recover from any unexpected data interruption.

LiveBallot employs multiple levels of monitoring, logging, and reporting . Primarily, the monitoring agent (MA) gathers monitoring and diagnostic log information from many places including the FC and the root operating system (OS) and writes it to log files. It eventually pushes a digested subset of the information into a pre-configured Windows Azure Storage Account. In addition, the Monitoring Data analysis Service (MDS) is a freestanding service that reads various LiveBallot monitoring and LiveBallot diagnostic log data and summarizes/digests the information, writing it to an integrated log.

LiveBallot Audit Logs

The LiveBallot audit logs of critical servers within hosting infrastructure, such as domain controllers, security servers, and servers containing sensitive information are collected near real-time via the System Center Operations Manager 2007 Audit Collection Services (ACS)

feature and stored in a SQL Server database. Due to the large amount of data collected for these environments, important and relevant events (referred to as "Events-of-Interest") are extracted and forwarded to another SQL database where OSSC uses automated tools to perform detailed analysis looking for suspicious activity. The information collected from the event logs includes user logon, security policy configuration changes, and unauthorized access to system or application files. As with the records generated by perimeter and network devices, the Events-of-Interest extracted from the LiveBallot audit logs are reviewed for evidence of control failure, unauthorized modification of server configuration, and other malicious activity.

Security of Data

Security of the balloting data is of utmost importance to Democracy Live team. LiveBallot employs many of the world's leading security and encryption experts and has dedicated hundreds of millions of dollars into the area of IT security. With tens of millions of transactions per month, the secure Microsoft cloud computing environment has proven to be an extremely stable and secure hosting platform.

The hosting environment undergoes annual audits for PCI DSS, SOX and HIPAA compliance, as well as internal assessments throughout the year. The hosting environment has obtained ISO/IEC 27001:2005 certification and SAS 70 Type 1 and II attestations. The cloud environment is ideal for load balancing, taking advantage of additional capacity required by multiple instances of an application in a manner that is efficient in terms of configuration and deployment. Cloud-based architecture provides elasticity, the ability to expand and contract capacity on-demand allowing the architecture to scale and meet those demands.

System hosting protection

LiveBallot uses industry standard access mechanisms to protect the application and its data located in the datacenter facilities. Access is limited to a very small number of operations personnel, who must regularly change their administrative access credentials. Datacenter access, and the authority to approve data center access, is controlled by operations personnel in alignment with local data center security practices.

Each data center facility has a minimum of two sources of electrical power, including a power generation capability for extended off-grid operation. Environmental controls are self-contained and remain operational as long as the facility and contained systems remain online.

Physical security controls are designed to "fail closed" during power outages or other environmental incidents. In case of fire or situations that could threaten life safety, the facilities are designed to allow egress without remaining exposed.

Risk to Ballot and Data Security though use of Email Ballot Delivery

Email is vulnerable to both passive and active attacks. Passive threats include *Release of message contents*, and *Traffic analysis* while active threats include *Modification of message contents*, *Masquerade*, *Replay*, and *Denial of Service (DoS)*. Actually, all the mentioned threats are applicable to the traditional email protocols,

- **Disclosure of Information**: Most emails are currently transmitted in the clear (not encrypted). By means of some available tools, persons other than the designated recipients can read the email contents.

- **Traffic analysis**: It is believed that some countries are routinely monitoring email messages as part of their surveillance. This is not just for counter-terrorism reasons but also to facilitate combat against industrial espionage and to carry out political eavesdropping. However, it is not devoted to the national agencies since there is a thriving business in providing commercial and criminal elements with the information within emails.

- **Modification of messages**: email contents can be modified during transport or storage. Here, the man-in-the-middle attack does not necessarily require the control of gateway since an attacker that resides on the same Local Area Network (LAN), can use an Address Resolution Protocol (ARP) spoofing tool to intercept or modify all the email packets going to and from the mail server or gateway.

- **Masquerade**: It is possible to send a message in the name of another person or organization.

- **Replay of previous messages**: Previous messages may be resent to other recipients. This may lead to loss, confusion, or damage to the reputation of an individual or organization. It can cause some damage if email is used for certain applications such as funds transferring, registration, and reservation.

- **Spoofing**: False messages may be inserted into mail system of another user. It can be accomplished from within a LAN, or from an external environment using Trojan horses.

- **Denial of Service**: It can put a mail system out of order by overloading it with mail shots. It can be carried out using Trojan horses or viruses sent to users within the contents of emails. It is also possible to block the user accounts by repeatedly entering wrong passwords in the login.

Because email connects through many routers and mail servers on its way to the recipient, it is inherently vulnerable to both physical and virtual eavesdropping. Current industry standards do not place emphasis on security; information is transferred in plain text, and mail servers

regularly conduct unprotected backups of email that passes through. In effect, every email leaves a digital paper-trail in its wake that can be easily inspected months or years later.

LiveBallot - Reporting

Post Election Reporting

Voter information and election data uploaded to LiveBallot are safely stored on the Microsoft Secure eGovernment Cloud Platform and is protected by 228-bit access and view applications and data running on the secure servers.

Localities that receive grant funding from the Federal Voter Assistance Program must be able to generate statistical reports that measure the effectiveness of electronic ballot delivery to military and overseas voters. Because LiveBallot has been designed to support the efforts of FVAP grant recipients, these reports are included as part of the user experience for each of our customers.

All Democracy Live customers receive access to the LiveBallot reporting dashboard, along with training on how to access important statistical information. In addition to the dashboard, Democracy Live customers receive a complete file at the end of every election, with all information required by FVAP.

Sample Report as required by Federal Voting Assistance Program

Account Summary

Okaloosa County

	Active Duty Military Overseas	Spouse or Dependent of Active Duty Military Overseas	US Citizen Overseas	Active Duty Military Outside of County	Spouse or Dependent of Active Duty Military Outside of County	Unknown Voter Type	Total
Voter access	463	133	127	573	155	0	1451
Ballots downloaded	379	119	101	484	133	0	1216
Ballots downloaded multiple times by a user	182	68	43	182	47	0	522
Ballots downloaded from domestic IP address	325	72	45	484	133	0	1059
Ballots downloaded foreign IP address	54	47	56	0	0	0	157

Question #5 (License Agreement)

Will my County be responsible for paying for this project?

Answer – No.

The License Agreement is between Rockwall County (as the Consortium leader) and the vendor alone. It reflects the approved grant amount that has been approved by the Federal Voting Assistance Program. Participating counties are not required to have a separate agreement.

Invoicing
Democracy Live will provide project invoices the County for purposes of submission to the Federal Voting Assistance Program (DoD). All license fees and program costs will be paid with federal funds. The County will bear no financial responsibility for the term of the contract.

Funding
The agreement between the parties is contingent on the award and funding support provided though the Federal Voting Assistance Program (DoD) EASE 2.0 Grant.

Term
The initial term for the Agreement, including Support and Maintenance, will be five years, commencing on the Effective Date of the Agreement, and will renew automatically on each Anniversary of the effective Date, provided that County may terminate the Annual License by notifying Democracy Live in writing at least sixty (60) days in advance of the renewal date. The Agreement, including Support and Maintenance, will terminate if the Agreement expires or is terminated.

Question #6

When will we know if the grant is approved?

Answer – Approved.

The approval for the grant from Mr. Bob Lavelle, Grant Officer is included and the grant amount is in the License Agreement.

Approval by the Federal Voting Assistance Program

Rockwall County leads the *Your Texas – Your Vote, which is the largest consortium of grant applicants in the United States to be awarded funding by FVAP. The Rockwall County Elections Administrator has reached an agreement with the Grant Administrator to finalize the award allocation:*

From: Lavelle, Bob J CIV DHRA [mailto:Bob.Lavelle@osd.pentagon.mil]
Sent: Thursday, August 15, 2013 1:33 PM
To: 'gdenton@rockwallcountytexas.com'; Burgess, Robin CIV WHS-FVAP
Subject: Re: Grant

Glenda: the most recent revision of your budget is acceptable. I plan on having terms and conditions to you and all other grantees by end of next week.

Bob Lavelle
Grants Officer

Note: The standard Terms and Conditions that are provided by FVAP are written into the agreement between Democracy Live and Rockwall County. It is the desire by the Grants Officer to have the contract executed before September 20th 2013, due to the end of the Federal fiscal calendar.

Conclusion

Sample Ballot Delivery

The LiveBallot Sample Ballot technology gives any voter, regardless of ability, access to an online, audio-enabled, voter specific sample ballot. LiveBallot allows every voter an equal opportunity to learn about the candidates and issues appearing on the ballot before they go to the polls. Access to a sample ballot will help all voters be better informed and will increase participation levels among voters with disabilities.

Military and Overseas Ballot Delivery

Rockwall County leads a consortium of 50 Texas counties, representing more than 15,500 Military and Overseas Texans by applying for and being awarded the fully-funded Federal Voting Assistance EASE 2.0 Grant. The name of our Consortium is *Your Texas – Your Vote.* The goal of *Your Texas – Your Vote* is to provide greater access to online services and tools in order to make the voting process easier and simpler for our growing population of Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) voters.

I am asking for the Court's approval to accept the Interlocal Agreement that will allow the County participate the Texas Effective Absentee Systems for Elections (EASE) Grant project t. This grant will help 50 Texas Counties to provide greater access to online services and tools in order to make the voting process easier and simpler for our growing population of military and overseas voters.