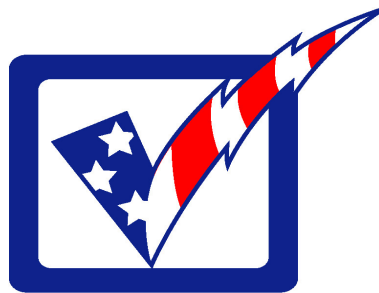# Department of Defense
Washington Headquarters Services
Federal Voting Assistance Program

Voting Over the Internet
Pilot Project
Assessment Report

June 2001

The Voting Over the Internet (VOI) Pilot Project was a groundbreaking event. In addition to being a successful technology proof-of-concept, the VOI Pilot was an exemplary case study of effective collaboration by Federal, state, and local government; industry; and private citizens. This project spanned more than 2-1/2 years of hard work and dedicated effort by the Federal Voting Assistance Program (FVAP), state and local election officials, and supporting Department of Defense (DoD) agencies. We were also assisted by a group of volunteers from the Uniformed Services community and overseas citizens who made history by being the first to register and cast their votes over the Internet in a Presidential election. Booz·Allen & Hamilton did an outstanding job of assisting the FVAP in defining the concept for this pioneering effort, in designing and implementing an innovative system, and in assessing project results. Computer Sciences Corporation helped us break new ground in defining testing standards where none existed before.

I thank all the people who made this project a resounding success. A special thanks to the Director, Administration and Management/Director, Washington Headquarters Services, and other DoD officials for helping the FVAP realize its vision of finding secure technological solutions to further enfranchise our absentee Uniformed Services and overseas citizens.

Additionally, we could not have completed this project without the shared vision and enthusiastic support of the election officials in the States of South Carolina, Florida, Texas, and Utah; and in Okaloosa and Orange Counties, Florida; Dallas County, Texas; and Weber County, Utah. As essential partners on our VOI project team, they defined what the Pilot System needed to do and ensured that all election administration standards were met and procedures followed.

The VOI volunteer citizens—a very special group of people—were the first users of two pilot programs: the VOI and the DoD Public Key Infrastructure. These users provided invaluable feedback that will contribute significantly to the development of future remote Internet registration and voting. They realized the potential of this technology to make absentee voting more accessible and were willing to contribute their individual efforts to help make it happen.

Finally, I want to recognize the VOI development team for their extraordinary efforts in meeting all project objectives, including preserving the integrity of the electoral process, and ensuring that the Pilot System was fielded on schedule for the November 2000 Presidential Election. All of these individuals have demonstrated that with a shared vision, a sense of urgency, and a focus on success, a vision can be realized.

Polli Brunelli
Director

TABLE OF CONTENTS

EXECUTIVE SUMMARY

For several years there has been growing interest in using Internet technology to make voting more accessible and convenient. A category of citizens who have experienced difficulties in participating in elections are those persons covered under the *Uniformed and Overseas Citizens Absentee Voting Act* (UOCAVA). By definition, these citizens are unable to go to the polls in person either because they have been assigned to duty stations away from their place of voting residence or are living outside the United States. The Federal Voting Assistance Program (FVAP) under the Department of Defense (DoD) administers this *Act* on behalf of the Secretary of Defense, who is the Presidential designee for carrying out the Federal provisions. In the pursuit of identifying ways to maximize access to the polls for these citizens, the FVAP and a group of state and local election officials conducted a small-scale pilot project to examine the feasibility of using the Internet for remote registration and voting for UOCAVA citizens. This report presents the assessment results of the Voting Over the Internet (VOI) Pilot Project.

The Pilot Project was implemented for the November 2000 General Election. Ninety-one military service members, their dependents, and overseas citizens used the Pilot System to register to vote absentee; 84 citizens voted using the VOI System. These citizens were located in 21 States and 11 countries. This was the first time that binding votes were cast over the Internet for Federal, state, and local offices, including the President and members of Congress.

The VOI Pilot was a cooperative Federal, state, and local government project, with the FVAP acting as Program Manager. Participating election offices were the States of Florida, South Carolina, Texas, and Utah; and local election officials in Okaloosa and Orange Counties, Florida; Dallas County, Texas; and Weber County, Utah. The Pilot System and procedures emulated the current UOCAVA absentee by-mail registration and voting process so that comparisons could be drawn between the two approaches. The roles and responsibilities of the participants remained the same as for the by-mail process. The Pilot System was fully compliant with all relevant Federal and state legal requirements.

Section 1 of this report describes the project background, identifies the participants and scope, provides a description of the Pilot System, and describes how the Project was conducted. The States of Florida, Texas, and Utah specified particular counties to participate; the State of South Carolina chose to make the Pilot available to any UOCAVA citizen in the State. A custom-designed computer system was developed and fielded at the local election offices. State and local election officials worked with the FVAP to identify the capabilities needed to enable citizens to use personal computers to remotely register and vote absentee over the Internet from their homes or workplaces. Digital certificates and encryption were used to provide privacy and security for all citizen and LEO transactions. The System was not designed to tabulate the returned ballots because it was intended to replicate the by-mail UOCAVA process. It was also designed without automated interfaces to other election administration systems, such as tabulation systems, so that the security perimeter of the System could be clearly defined for testing purposes. Prior to tabulation of the ballots, the local election officials used a controlled process to decrypt and print the electronic ballots, and transcribed them to absentee ballots which were entered into the local tabulation system.

Section 2 describes the methodology used to assess the results of the VOI Pilot Project. The purposes of the assessment were to—

- Assess whether electoral process integrity was maintained and a secure and transparent process was achieved

- Determine if the Pilot improved UOCAVA citizen access

- Consider the implications of scaling from a small Pilot to a larger system

- Provide information to assist the FVAP and state governments in determining what further steps to take for Internet registration and voting.

To provide a baseline for understanding the assessment results, Section 3 provides a comparison of the by-mail and VOI processes for UOCAVA remote registration and voting. "Remote" registration and voting means that the citizens are doing these activities from their homes or workplaces, and not at a location operated by a local election office. Each major activity is described in step-by-step detail, explaining the actions performed by citizens and local election officials.

The biggest question regarding the use of the Internet for registration and voting is whether the integrity of the electoral process can be preserved. There are a number of elements to be considered relative to whether this technology can provide sufficient security, secrecy, and transparency of the process to be relied upon for the exercise of this most fundamental of Constitutional rights. Another major concern is the potential for election fraud when using the Internet. Section 4 presents the project findings on process integrity and addresses whether this approach enhances the enfranchisement of this particular group of citizens and what new benefits, issues, and risks the technology introduces.

A principal finding of the assessment is that, within a small-scale, tightly controlled demonstration, the risks introduced by the technology can be sufficiently mitigated to maintain the integrity of the process for remote registration and voting. It was also shown that this approach has the potential to significantly promote the enfranchisement of UOCAVA voters, in particular, military service members. However, further considerations include whether the VOI Pilot System concept is sufficiently mature to move to a fully operational environment and how well the System would scale from fewer than a hundred voters to tens of thousands. Section 5 presents the lessons learned from the project and briefly discusses the principal scalability issues.

In conclusion, further development is needed before Internet remote registration and voting can be provided effectively, reliably, and securely on a large scale. This report concludes with Section 6, which outlines the FVAP recommendation. The next development project would provide a remote registration and status-checking capability and focus on working out the issues of scalability and fuller integration with local election office systems and procedures in one or more states. At the same time, research would continue on identifying solutions for the security issues related to actually casting ballots over the Internet for voting on a large scale. The FVAP would also continue working with state election officials on legislative initiatives and with the Federal Election Commission and other standards organizations on the development of standards.

1.0 VOTING OVER THE INTERNET (VOI) PILOT PROJECT OVERVIEW

1.1 BACKGROUND

The *Uniformed and Overseas Citizens Absentee Voting Act* (UOCAVA)[1] protects the right to vote for federal offices by absent Uniformed Services and overseas citizen voters. By definition, these categories of voters are absent from their place of voting residence and unable to vote in person. The *Act* prescribes the establishment of uniform absentee forms and procedures to accommodate the special circumstances of these citizens thereby facilitating their Constitutional right to vote. The Secretary of Defense is the Presidential designee responsible for the Federal functions of the *Act*. The Federal Voting Assistance Program (FVAP) administers this law on behalf of the Secretary of Defense and works cooperatively with state and Local Election Officials (LEOs) to carry out its provisions.

After each Presidential election, the FVAP conducts a survey of UOCAVA citizens to gather information about their participation. These surveys have demonstrated consistently that mail transit time is a significant barrier to their ability to vote. Through the years, the FVAP and state election officials have launched a number of initiatives aimed at reducing this barrier. For example, special envelope designs have been developed to allow easy identification of election-related mail and promote expedited processing. In addition, as a result of the successful emergency use of facsimile technology for military voting during Desert Shield/Desert Storm, 46 states permitted the use of facsimile for transmission of election materials at the time of the November 2000 Presidential Election.[2]

While facsimile is a useful alternative to the by-mail process, it has two major drawbacks: it does not allow for secrecy and it is not universally available at local election offices. As the Internet became increasingly ubiquitous and widely accepted by the public, it was a natural evolution for the FVAP and the states to consider the potential of this technology. Through a series of meetings and discussions with state and local officials, the decision was made to conduct a small pilot project to assess the feasibility of using this technology as an alternative to the by-mail process for absentee UOCAVA registration and voting. Several states volunteered to participate, funding was acquired, and the project was formally launched in August 1998.

The goal was to examine the feasibility of using the Internet as an alternative method for remote absentee registration and voting for UOCAVA citizens through a small-scale pilot project. This report documents the results of the project assessment. The assessment was scoped to consider the technical performance of the system, as well as its ability to meet the requirements of maintaining the integrity of the electoral process, providing an acceptable level of security, being easy to use for both citizens and elections officials, and meeting all the legal requirements for a voting system.

---

1   UOCAVA (42 U.S.C. § 1973ff) permits absent members of the Uniformed Services, merchant marine, their eligible family members, and U.S. citizens residing outside the United States, to use absentee registration procedures and to vote by absentee ballot in general, special, primary, and runoff elections for federal offices.

2   Of these 46 states, 23 allow faxing of blank ballots to voters and 17 allow voters to return voted ballots by fax. Nine of the 17 states restrict the use of facsimile to military personnel, or to emergencies and special cases, or to overseas voters. Eight have not placed restrictions on the faxing of voted ballots.

1.2 PILOT PROJECT JURISDICTIONS

The VOI Pilot Project was a cooperative Federal, state, and local effort. The FVAP was the Program Manager; the participating state jurisdictions were Florida, South Carolina, Texas, and Utah.[3] The State of South Carolina chose to make the VOI process available to all UOCAVA voters from that state, regardless of their county of voting residence. The other states had specific counties that volunteered to participate. These were Okaloosa and Orange Counties in Florida, Dallas County in Texas, and Weber County in Utah.

In addition to their different demographics, these participating jurisdictions presented a variety of election administration environments. The State of South Carolina and Dallas County, Texas, had to request Department of Justice preclearance approval for this proposed change in their election administration procedures. Dallas and Orange Counties had to provide ballots in both English and Spanish. Some of these jurisdictions required the option to vote a straight party ticket. Florida required the ability to notify the voter that he or she had voted for too many or too few candidates in a particular race. Two different candidate write-in procedures were used. Texas limited the use of electronic transmission for voting to military personnel in designated combat zones, or in hostile fire or imminent danger pay areas.

1.3 PILOT PROJECT SCOPE

The participants decided at the outset of the VOI Project that the ballots cast using the System would count. It was agreed that operating in "mock" election mode would weaken the significance of the results and thus devalue the utility of the effort. Every aspect of the UOCAVA absentee registration and voting process was duly considered and fully incorporated into the design and operation of the Pilot. In keeping with this philosophy, the Pilot System and procedures emulated the absentee by-mail process. Therefore, the roles and responsibilities of the Federal, state, and local government participants did not change, and the Pilot was fully compliant with all relevant Federal and state legal requirements.

A number of operating principles were agreed upon for the VOI Pilot. First, the System had to comply with all Federal and state legal and procedural requirements. The integrity of the electoral process, one person-one vote, and the secrecy of the ballot had to be maintained, and the ability to fully audit the process was required. The respective roles and responsibilities of the FVAP, the states, and the LEOs were not to change. The Internet-based system would be designed to emulate the by-mail process as closely as possible so a meaningful comparison could be made. Volunteer citizens could access the System from personal computers at their homes or workplaces. The VOI voting period would extend from the date of availability of absentee ballots through the close of polls in the participating jurisdictions. As a failsafe measure, volunteer voters were advised to use the by-mail process as a procedural back-up in the event the VOI System experienced an unanticipated outage or other operational problem.

The VOI Pilot Project was a small-scale, limited-scope feasibility study. It was small-scale in that only a few jurisdictions participated. There were a total of 15 counties (including 11 in

---

3 Missouri had identified two counties to participate, but subsequently withdrew from the project because of staffing limitations.

South Carolina), which is a very small percentage of the more than 3,000 counties in the United States. It was also small-scale because of the number of voters who volunteered. At the beginning of the project, the participating states identified 50 as the maximum number of voters who could be accepted from any single jurisdiction. Their rationale was that this number was large enough to provide a good test of the concept, but small enough so as not to affect the outcome of any electoral race.

Although a number of process improvements would have been possible, the VOI System was intentionally designed to mimic the absentee by-mail process to enable valid comparisons between the by-mail and the Pilot alternative. For this reason, the System was not designed to tabulate, but to produce only printed paper ballots. Because the VOI Pilot was limited in scope and was intended to be a proof-of-concept system, only the minimum essential effort was expended in optimizing design and software applications. For example, the System was built to interface only with citizen personal computers running a Microsoft Windows 95/98™ operating system with a Netscape Navigator™ browser. Macintosh™ or UNIX™ platforms could not be used, nor could Microsoft Internet Explorer™.

In addition, the VOI System was intentionally designed as a stand-alone system without automated interfaces to other election administration systems at the local election offices, such as the voter registration database. This decision resulted from the need to conclusively define the security perimeter of the System to allow meaningful certification and accreditation testing. When considering remote registration and voting via the Internet, the primary concern is whether an appropriate level of security can be achieved. Therefore, the ability to have very clear findings relative to security was a key pilot design consideration.

Finally, the scope of the VOI Pilot was limited in that it was designed for use only for the November 7, 2000, General Election. However, this does not mean that the VOI System was used only on that day. The VOI absentee voting period was approximately 30 days from the date of ballot availability until the close of polls. Pilot citizens also used the System to register to vote absentee and be eligible to receive a ballot.

The VOI Pilot timeline differed from the absentee by-mail process in only one respect. Florida, Texas, and Utah permit military absentee ballots to be counted for a specified period after election day, as long as the ballots are postmarked from overseas before the close of polls.[4] The reason for this practice is to allow a grace period to compensate for the by-mail delivery time from overseas. Given that delivery over the Internet is virtually instantaneous, there was no need to extend the ballot acceptance period. Consequently, the VOI process used the same "close of polls" rule as in-person voting.

1.4 VOI SYSTEM ARCHITECTURE HIGH-LEVEL OVERVIEW

As illustrated below in Figure 1.4-1, the VOI Pilot System was comprised of three major components: citizen workstations, an FVAP server segment, and a LEO server segment. The

---

4   At the time of the November election, in Florida, the Federal portion of the voted ballot was counted if it was postmarked or dated no later than the day of the election and received up to 10 days after the general election. In Texas, the voted ballot must be placed in delivery by 7:00 p.m. on election day so that it arrives no later than 5 days after the general election. In Utah, the ballot must be returned so that it arrives by noon on the Monday after the election.

basic functions of this System were to permit Pilot citizens to register, vote, and check their registration and voting status from their homes or workplaces.

Figure 1.4-1. Diagram of the VOI System Architecture
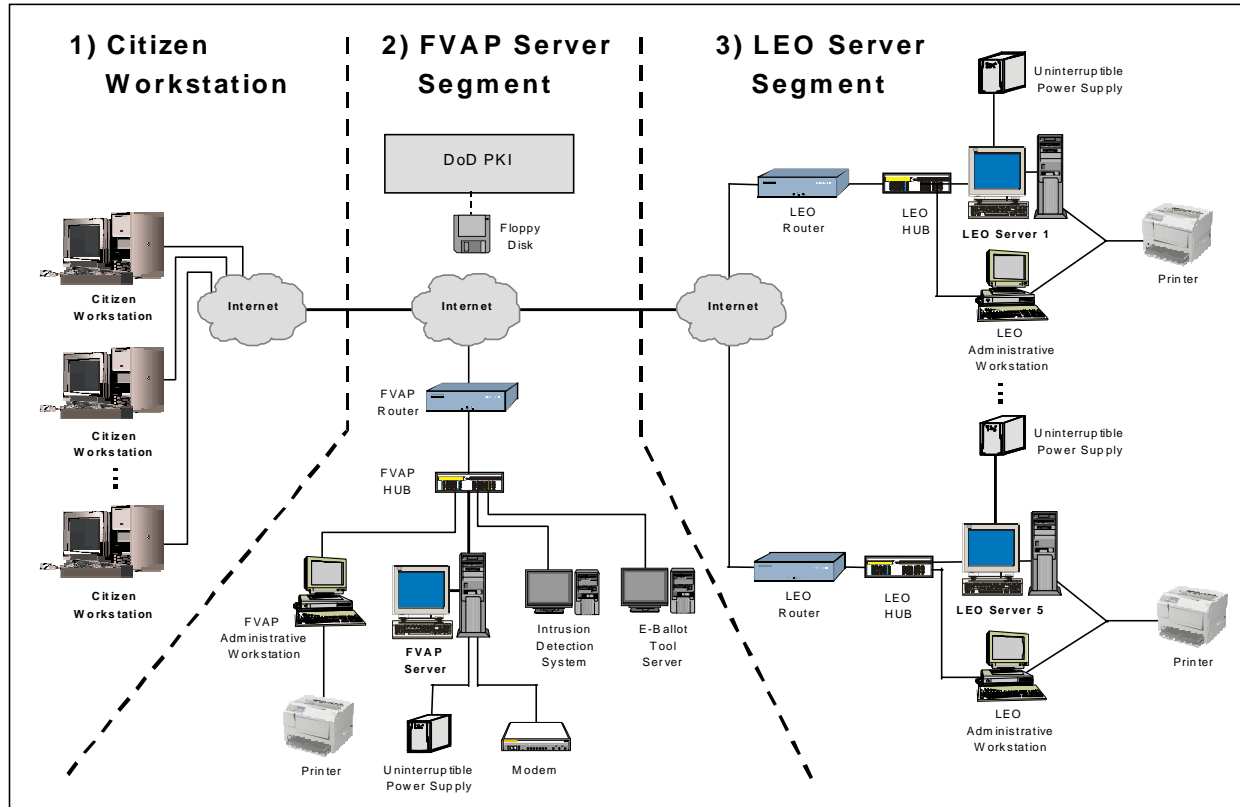
Source: VOI Security Architecture Document

The citizen workstation was a personal computer with Internet access that the volunteer Pilot citizens had available at work or at home. The FVAP and LEO segments were dedicated to the VOI System. The E-Ballot Tool Server provided the capability for LEOs to generate electronic ballots. The Department of Defense (DoD) Medium Assurance Public Key Infrastructure (PKI) was a separate system that managed digital certificates and certificate revocation lists for all PKI-enabled DoD applications. Communications connectivity between the FVAP, LEO, and Pilot citizens was conducted via the Internet.

1.4.1 Citizen Workstation

The citizen workstation was the computing platform used by participating citizens to access the Pilot System from their residences or workplaces. The performance requirements for the workstations were intentionally modest to ensure that most existing personal computers would be compatible. The minimum requirements were that the citizen workstation run a Microsoft Windows 95/98 operating system, have a connection to the Internet, and have the Netscape Navigator browser (Version 4.05 or higher, with strong encryption) installed to provide a graphical user interface to the VOI System. Macintosh or UNIX platforms could not be used, nor could Microsoft's Internet Explorer browser. Custom software to enable VOI-specific

functionality, in the form of a browser plug-in, was included on a CD-ROM sent to each citizen by the FVAP. The CD-ROM also included the strong encryption (128 bit) version of Netscape Navigator for those citizens who needed to upgrade their browser software to be compatible.

1.4.2 FVAP Server Segment

The FVAP server segment was the central component of the VOI System, providing the link between the citizen workstations and the LEO servers. The FVAP server segment included several different computing platforms, network communication components (router, hub), and other components, including a printer, an uninterruptible power supply, and a modem for paging system operations and maintenance staff. The FVAP segment included the FVAP server, two intrusion detection systems, the E-Ballot Tool server, and the FVAP administrative workstation. The administrative workstation is a personal computer running a Netscape Navigator browser client and is the principal interface to the FVAP server for system performance monitoring activities. The two intrusion detection system components were positioned on the outside and inside of the filtering router to monitor network activities and identify suspicious behavior. The intrusion detection system located outside the router is not depicted in the system architecture diagram. These two components, along with the filtering router and configuration changes to the FVAP server's Microsoft Windows NT™ operating system all combined to make the FVAP segment an important security barrier protecting the Pilot System.

FVAP Server

The FVAP server included a highly reliable computer hardware server, its operating system, database management software, application server software, and the VOI custom-developed software. From a functional perspective, the FVAP server identified and authenticated users, allowed users to transfer Electronic Federal Post Card Applications (EFPCAs) and E-Ballots to and from the LEO servers, and performed "postmarking" functions. The content of all transactions passed through the FVAP server in encrypted form so only the addressing information could be read for communications routing purposes.

E-Ballot Tool Server

The E-Ballot Tool server was located within the FVAP server segment security architecture and access to it was restricted to specified LEO staff via an access control list. This server was dedicated to hosting the E-Ballot Tool software. The LEOs used this software to build their electronic ballots. After all the component files for the ballots were defined, the LEO would copy those associated with a specific ballot style to a floppy disk and upload them to the LEO server. No ballots were stored on the E-Ballot Tool server.

1.4.3 LEO Server Segment

Each LEO site had a server that provided connectivity only from the FVAP server via the Internet to transmit or receive EFPCAs, E-Ballots, and status messages. Each LEO segment included the server hardware platform, the Microsoft Windows NT operating system, the VOI custom software, a printer, a removable storage media unit, uninterruptible power supply, and network communications devices. Like the FVAP segment, each LEO segment had an additional workstation for administration of the LEO server.

1.4.4 DoD Medium Assurance PKI

The DoD Medium Assurance PKI is a separate system from the Pilot System. The VOI System required support from the DoD PKI for electronic certificate registration and management services. Two components were needed: the Certification Authority and the Directory Server. The Certification Authority issued the digital certificates for all participants, which provided identity authentication within the VOI System. The Directory Server facilitated the certificate verification process by maintaining and providing the list of digital certificates that were no longer valid. Periodically, the certificate revocation list was manually downloaded from the DoD PKI directory to a floppy disk for manual transfer to the FVAP server.

1.5 COST OF THE VOI PILOT PROJECT

The cost for defining, developing, operating and assessing the VOI System for remote Internet registration, voting, status checking, and post-election processing of ballots in the November 2000 General Election was $6.2 million. It should be noted that the cost of a proof-of-concept research and development project involving new technology applications is not equivalent to the cost of owning and operating a system in the normal course of business.

The project funding encompassed a wide variety of activities as well as the purchase of the System hardware and commercial software for all the participating locations. In addition, the equivalent of four full-time government personnel provided program management and oversight; coordinated with state and local election officials, the Department of Justice, the DoD PKI Program Management Office, and military services representatives; issued digital certificates; recruited and tracked citizen volunteers; and disseminated system software and documentation.

The following elements are included in the cost of the VOI Pilot—

- A comprehensive analysis and definition of System functional requirements for the four states that participated in the Pilot. While there is considerable similarity in how UOCAVA registration and voting is conducted nationwide, there is still some variability in timelines, ballot formats, and other election administration aspects of the process that are defined by state election codes and administrative procedures.

- Extensive coordination with both state and local election officials throughout the development of the System requirements, architecture, processes and procedures, and software; and the carrying out of the System integration, testing, installation, certification, operation and assessment.

- An architecture design process that included the development of alternative technical solutions for assessment and selection.

- Hands-on demonstrations of various capabilities provided to the LEOs during the software development process to ensure the final products would satisfy their needs when the System was fielded.

- Procurement of commercial off-the-shelf (COTS) hardware and software for each of the five LEO locations and the FVAP, and separate environments for the development, test,

and operational systems. Hardware and software were also procured to support the E-Ballot Tool.

- Custom software development that supported—
  – Software interfaces with PKI systems for processing Medium Assurance identity and privacy certificates
  – Registration by the citizen
  – Registration object transport through the FVAP server to the appropriate LEO server and processing of the citizen registration by the LEO
  – Citizen Status Checking capability
  – Building of blank ballots by the LEOs through the use of the E-Ballot Tool
  – Citizen blank ballot request and object transport
  – Citizen ballot voting, encryption, and transport to the FVAP server for citizen identification and authentication, "postmarking," and transport to the appropriate LEO server
  – Voted ballot processing by the LEOs including ballot reconciliation, voter identity removal, ballot decryption, ballot printing, and data archiving.

- System integration, installation, and testing of the four major components of the VOI Pilot System: Citizen software, the FVAP server, E-Ballot Tool server, and the LEO servers, at six geographically dispersed locations.

- Preparation of system documentation and user documentation (e.g., *Citizen Guide*, *LEO Administrator's Manual*, *Electronic Ballot Tool Manual*, the *FVAP Administrator's Manual*).

- Training of LEO personnel on the use and operation of the VOI System and the E-Ballot Tool.

- Two independent test and certification processes, one for DoD and the other for the State of Florida. This included the development of test criteria and procedures. The testing was performed in the development lab and at two LEO locations.

- Operation of the FVAP server site, manning the Help Desk, and monitoring and troubleshooting the total operational system (the FVAP server, E-Ballot Tool, and five LEO servers).

- Post-election assessment of the VOI Pilot Project including a functional and technical assessment of system performance, ease of use, and meeting of program objectives. The assessment was conducted with the participation of both the volunteer voters and the LEOs.

1.6 CONDUCT OF THE PILOT PROJECT

1.6.1 Pilot System Development

The FVAP relied extensively on the knowledge and experience of the states and LEOs to define the absentee registration and voting requirements for the VOI Pilot System. Under the U.S. Constitution, each state government determines the times, places, and manner of holding

elections in their state. The execution and administration of elections according to these rules is carried out at the local level. The VOI development team spent several months in early 1999 reviewing state laws and election administration documentation and meeting with election officials to capture the basic VOI System requirements. These requirements were documented and circulated to the LEOs for review and comment.

As system development progressed, the LEOs were contacted frequently by phone and e-mail for clarification regarding these requirements. In addition, the LEOs were given the opportunity to preview the system and make comments and suggestions at three major milestones: September 1999, when the registration application was near completion; May 2000, when the E-Ballot Tool was near completion; and June 2000, when the voting application was near completion. Each review resulted in further fine-tuning of the Pilot System capabilities.

1.6.2 Implementation of the FVAP and LEO Systems

The implementation of the VOI System was conducted in two phases. The FVAP and LEO hardware suites and the absentee registration application were deployed in December 1999 and a semi-automated Check Status feature was added in June 2000. The voting application and the fully automated version of the Check Status feature were deployed during the months of September and October 2000. Third-party testing and DoD security certification and accreditation were completed in December 1999 for the first phase of the System. Third-party testing, DoD certification and accreditation, and State of Florida certification were completed in September 2000 for the full system.[5]

Absentee Registration Application

Under current provisions in many states, UOCAVA citizens may submit an absentee registration and ballot request application in January of each year. In most states, this serves as an absentee ballot request for all elections in that calendar year for which the voter is eligible. Because the VOI process mirrored the absentee by-mail process, it was determined that the VOI System should be available for electronic registration in January 2000. To meet this operational date, the registration application was implemented on the FVAP server in November 1999, followed by deployment of the System to all the LEO sites in December 1999.

Because the FVAP disseminates the FPCAs for the by-mail process, the blank EFPCAs were stored on the FVAP server and delivered electronically upon citizen request. While the paper FPCA form is a standard format of informational fields for use nationwide, each state specifies which fields are required to be completed and which are considered desirable, but not mandatory. The FVAP publishes and disseminates the *Voting Assistance Guide* (VAG) as an informational aid that describes each state's specific instructions, procedures, and timelines for the submission of this form. The VAG and FPCA forms are distributed to Voting Assistance Officers located worldwide at military installations, embassies and consulates, and overseas citizen organizations. In the absentee by-mail process, the UOCAVA citizen obtains an FPCA form from a Voting

---

5   The testing and certification process is discussed in Section 1.6.4.

Assistance Officer and can refer to the VAG for an explanation of how to complete it.[6] To facilitate the VOI process, the blank EFPCAs were tailored to reflect the specific instructions of each of the participating VOI Pilot states, thereby eliminating the need for the citizen to refer to the VAG.

Following the implementation of the EFPCA software application on the FVAP server, the VOI System hardware and software were deployed to all LEO sites. The development contractor installed, configured, and tested each LEO system. The LEO personnel observed all of these activities. As each system was tested and deemed operational, the LEO personnel were individually trained to operate the system and process EFPCAs. A LEO User Manual was also provided. Following the completion of training, the system was released to the LEOs for operation.

Semi-Automated Check Status Feature

In June 2000, the Check Status feature was added on an interim basis to the FVAP server. This feature allowed the voter to access the System and inquire about his/her status (e.g., registration received, registration approved). The feature was semi-automated at this time, because it was added only to the FVAP server and not to the LEO servers. Until the Check Status feature could be installed on the LEO servers, the LEOs reported citizen status information to the FVAP weekly, and the data were manually entered into an interim application. The FVAP server responded to citizen queries. Because there were very few voters accessing the System at this time, this was an effective solution to providing status information.

E-Ballot Tool Application

The original VOI System plan called for the development of an E-Ballot specification to define the parameters for creating the E-Ballot formats needed for the VOI System. This document would provide instructions for the LEOs when constructing electronic versions of their paper absentee ballots. As software development proceeded, it became obvious that this approach by itself was too high-risk. The FVAP became concerned that errors in manually generated E-Ballots discovered too close to election day would endanger the success of the Pilot. In response to this concern, it was decided to develop a simple automated tool that would allow the LEOs to generate E-Ballots without detailed technical knowledge.

As this effort progressed, the E-Ballot Tool became fairly complex because it had to accommodate the varied ballot requirements of the four VOI states. These included Spanish language ballots, straight party voting, straight party voting with exceptions, two different write-in procedures, the ability to notify the voter that he/she has over- or under-voted races or questions, and a variety of instruction formats (e.g., "vote for no more than two" or "vote for only two").

This application was installed on a separate secure server and could be accessed through the Internet from any LEO workstation. The tool was implemented in June 2000 and the LEO

---

6   An online version of the Federal Post Card Application and instructions for its completion are now available from the FVAP Web site as an alternative to the cardstock FPCA. However, it must be printed, manually signed, and sent via the mail so the registrant's signature is captured. At present, 45 states accept the online version.

personnel were provided a user's manual and trained. While requiring substantial additional development time and effort, this approach was highly successful. The E-Ballot Tool made it possible for the LEOs to construct and verify their E-Ballots, allowed the development team to obtain sample ballots early for testing, and did not produce any problems when the final ballots were loaded on the System and used.

Voting, Post-Election Processing, and Automated Check Status Applications

The voting, automated Check Status, and post-election processing applications were implemented at the LEO locations during the months of September and October 2000. Citizens were then able to log on to the VOI System to request and submit E-Ballots. With the fully automated Check Status feature, citizen inquiries were passed from the FVAP server to the appropriate LEO server and responses were automatically generated based on data in the EFPCA and ballot processing tables on those servers. This eliminated the need for any manual intervention by the LEO or FVAP personnel, while providing current status information with no reporting delays. The post-election processing application allowed the LEOs to validate the returned E-Ballots, separate voter identities, and decrypt and print the ballots. It also provided the ability to reset the System to allow for recounts if needed.

1.6.3 Pilot System Operation and Shutdown

The VOI System was operational and ready for use in late January 2000. The first successful registration was received from an Air Force voter from Orange County on April 16. The first voted ballot was received from a Marine Corps voter from Weber County on October 12, and was "postmarked" by the FVAP server at 3:39 p.m. Eastern Time. The last voted ballot was received from an Air Force voter from Orange County on November 7, 2000, and "postmarked" by the FVAP server at 5:53 p.m. Eastern Time. Figures 1.6-1 and 1.6-2 show the receipt of EFPCAs and E-Ballots over the course of the Pilot.

Recognizing the risks inherent in developmental systems, the FVAP determined early in the project that a back-up procedure had to be in place for Pilot voters. Consequently, voters who volunteered to use the VOI System were requested to register and submit a ballot via the absentee by-mail process. This was to avoid inadvertently disenfranchising the voter in the event of unexpected system outage or malfunction. In the instance where valid electronic and paper ballots were submitted, the participating LEOs adopted the practice of accepting and counting the E-Ballot. In this instance, the paper ballot was marked "duplicate" and not counted. In the event that an E-Ballot was not received, the paper ballot was counted.

To facilitate this process, each LEO established a procedure to identify the paper ballots returned from VOI voters so they could be held aside until ballot reconciliation. At that time, the LEOs determined if they had duplicate ballots and processed them accordingly. Checking for duplicate ballots is part of the LEO standard ballot reconciliation procedure and was not unique to the VOI Pilot process. Of the 84 E-Ballots returned, 74 were counted. The other 10 were not counted because the paper ballots from those voters had been deposited in sealed ballot boxes. There were 15 instances in which only E-Ballots were returned by voters.

Figure 1.6-1. Receipt of EFPCAs (April 2000 Through November 2000)
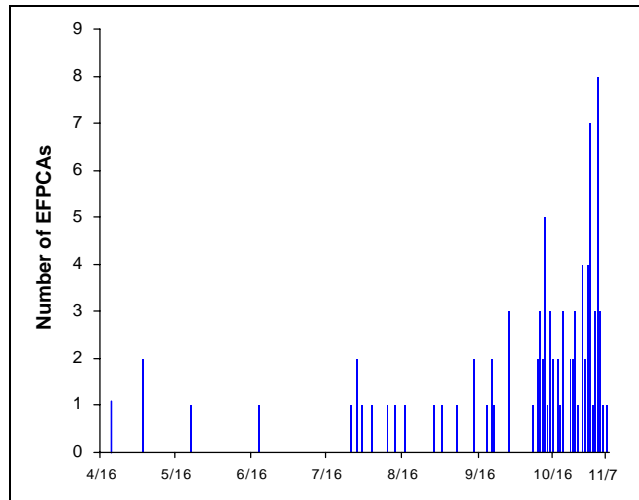
Source: FVAP Server Logs

Figure 1.6-2. Receipt of E-Ballots (October 2000 Through November 2000)
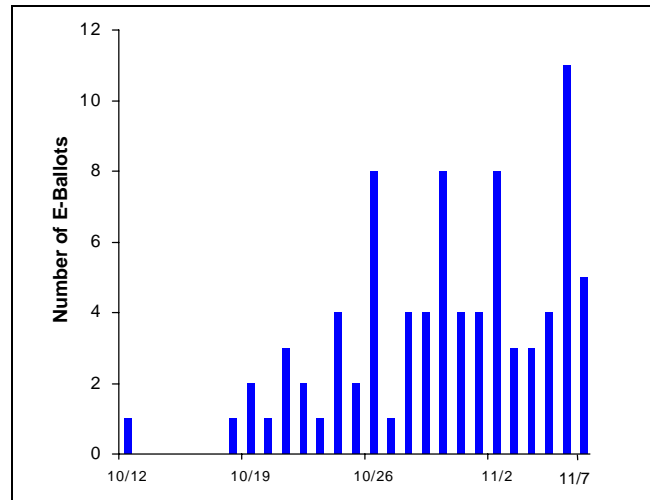
Source: FVAP Server Logs

While the Pilot System functioned well and the back up procedure did not have to be relied on for voting, these procedures saved the project from failure as a result of two developments totally unrelated to system performance. These were the unanticipated delays in identifying eligible volunteers and the unexpected difficulties experienced in getting digital certificates issued to the VOI voters.[7] As a result of these problems, many voters did not receive their digital certificates until after the deadline had passed for absentee registration. Their eligibility to vote in the November 2000 General Election was secured by the fact that they had submitted their absentee by-mail request within the prescribed registration period. While they still had to "register" on the VOI System, this only fulfilled the system registration requirement, which is an integral element of VOI System security. This explains why Figure 1.6-1 shows so many EFPCAs received after the 30-day pre-election registration deadline. The legal absentee voting application and ballot request requirement had been fulfilled by the paper FPCA.

Post-Election Shutdown

The LEOs disconnected their servers from the Internet shortly after the close of polls, when they were ready to do ballot processing. The VOI development team traveled to the LEO locations in December 2000, to assist in archiving the data from the servers in preparation for physical removal of the Pilot System.

1.6.4 Pilot System Testing and Accreditation

The VOI Pilot System underwent two certification processes, one prescribed by the DoD for information systems and the other prescribed by the State of Florida for voting systems.

---

7   These topics are discussed in Section 1.6.5, Pilot Voters.

VOI System Testing and Accreditation Process

The FVAP employed a third-party structured testing process to provide an independent validation of the VOI System's functional and security performance. The DoD has a well-established and defined testing process for information systems, the DoD Information Technology Security Certification and Accreditation Process. This process provides a comprehensive approach to characterize the anticipated threat scenario and the type and criticality of the system, so that the appropriate tailored testing procedures and standards can be applied.

The State of Florida requires that all voting systems be certified by the State Division of Elections before they can be used in any election. They have extensive written standards and test procedures that a system must comply with to be certified. The other VOI states also have voting system certification requirements, but they agreed to accept the results of the Florida certification process.

Tailoring the Test Requirements

While both the DoD and State of Florida standards and procedures were comprehensive, neither addressed Internet voting systems. Because this technology is fairly new to the DoD and cutting edge when it comes to voting systems, a considerable amount of time and effort was spent reviewing, revising, and adapting test procedures, first with the DoD testing group and then with the State of Florida certification experts. The VOI System Specifications and the Security Architecture documents provided the baseline for the system technical and functional requirements. Tailoring the testing activity entailed reviewing each test standard or procedure to determine if it could be directly applied to the VOI System. In those instances where the precise statement of the standard or procedure did not quite fit, the intent of the standard was considered and the language adapted to meet the intent. For example, it was determined that the Florida design, construction, and maintenance requirements for durable and reliable voting equipment were satisfied because the VOI System used all COTS equipment. However, in many instances, the standards did not apply. For example, the State of Florida mandates that FPCAs and ballots be printed on card stock that meets state standards and characteristics. This was not relevant for the VOI System because the election materials were in electronic form.

Conduct of Testing

The VOI Pilot System was tested in two phases. For the phase one deployment of the basic System and the registration application, only the DoD testing process was followed. When the voting application was ready to be deployed, the entire VOI System was tested using both the DoD and Florida standards.

The phase two testing was conducted on a test system configuration in the development laboratory and on the two operational systems in Orange and Okaloosa Counties, Florida. While there were a few anomalies detected in the testing, all the critical functionality and security features worked as required. The State of Florida completed its review of the testing results and issued two provisional certificates for the VOI Pilot System on October 17, 2000. Because the VOI System was not designed to tabulate, it was certified as an adjunct to the Accuvote and

Optech Voting Systems in use in Okaloosa and Orange Counties respectively. The certificates were provisional because the System was for one-time use for the November 2000 General Election.

1.6.5 Pilot Voters

The voters for the VOI Pilot were all volunteers and drawn almost entirely from the military services. The FVAP focused on military service members because the use of DoD Medium Assurance PKI digital certificates was essentially limited to this group. The organizational structure of the military services also provided more opportunity to disseminate Pilot recruiting information to potential volunteers than would have been possible with overseas government employees or private sector citizens.

Identification and Recruiting

The FVAP began the volunteer identification and recruiting effort in July 1999. The Service Voting Action Officers for the Army, Navy, Air Force, Marine Corps, Coast Guard, and the Department of State were individually contacted and briefed on the project. The FVAP requested the Voting Action Officers to notify their installations that the FVAP was looking for volunteers to participate in the Pilot. Sample messages were provided describing the project, the requirements for participation, and contact information.[8] Responses were requested by mid-September 1999. The FVAP also publicized the project and requested volunteers through the *Voting Information Newsletter* and the American Forces Information Service.

The Service Voting Action Officers used a variety of means to publicize the project. They sent official notifications to their respective Service units, placed articles in post newspapers and Service publications and posted announcements on Service home pages. Because the desired number of responses was not received by the original mid-September date, the deadline was extended as needed to meet the project goals. There was a large initial response to these announcements. However, because many volunteers were not voting residents of one of the participating jurisdictions, they had to be disqualified. Following this period, the identification of volunteers progressed slowly. As a result, other approaches were tried for Weber and Dallas Counties where the number of volunteers was the lowest.

Because only one volunteer had been identified for Weber County, Utah, by January 2000, an additional procedure was implemented. When the Weber County Clerk's office received FPCAs in the mail, the LEO forwarded the contact information to the FVAP. These voters were then contacted directly and asked if they would be interested in volunteering. This was a fairly successful approach, resulting in 13 additional volunteers.

Dallas County, Texas, posed the biggest challenge given the restrictive Texas legislative requirement that only personnel in designated combat zones, or in hostile fire or imminent danger pay areas are permitted to use electronic means for absentee registration and voting. No Dallas prospects developed until July 2000 when the Dallas County LEO notified the FVAP that a National Guard unit from the Dallas area had been mobilized to Bosnia. Repeated contacts

---

8   Eligibility to participate in the Pilot required volunteers to have a DoD Medium Assurance PKI digital certificate, be a
     voting resident of one of the participating jurisdictions, and have access to a PC connected to the Internet.

were made with this unit at various levels, including the Task Force Eagle Commanding General's office in Tuzla, Bosnia. It was determined, however, that this Guard unit would be returning to Texas before election day and therefore did not need to vote absentee. As a final measure, the LEO provided the FVAP a list of all absentee ballot requests received by the office. The FVAP reviewed this list for personnel who met the location requirement, and two voters in Turkey were identified and recruited for the project.

Okaloosa County, Florida, was the only jurisdiction where the number of volunteers exceeded the 50-person ceiling. To reduce the list, the LEO selected voters who were already permanently registered. A waiting list was maintained and several volunteers on the original list were replaced when they dropped out of contact with the project.

Identification and Recruiting Results

Of the 127 eligible voters identified, 104 were military service members, 19 were military spouses, and 4 were civilians. Ninety-one of the 127 eligible voters registered, and 84 returned voted E-Ballots.

Okaloosa County, Florida, had the largest number of participants: 38 voters registered and 38 voted. Orange County, Florida, had the second largest number of volunteers: 17 voters registered and 14 voted. In Weber County, Utah, 14 voters registered and 14 voted. While South Carolina had 21 voters register and 17 vote statewide, the largest number of participants in a single county was four. Dallas County, Texas, had only one person register and vote.

Issuing Digital Certificates

One of the principal requirements for the VOI Project was to be able to identify and authenticate voters with a high degree of certainty. The mechanism selected to provide this capability was the DoD Medium Assurance PKI. The issuing procedure for digital certificates required the recipient to appear in person before an issuing authority or the authority's trusted agent and present official photo identification. After receiving and signing the certificate document, the participant had to "fulfill" the certificate by accessing the PKI Web site and downloading his/her certificate to a floppy disk. The participant also had to assign a password to his/her digital certificate.

The DoD PKI program was a separate development program from the VOI System. Early in the VOI Project, the FVAP committed to the use of the DoD certificates, and the PKI Program Management Office (PMO) agreed to issue the certificates to the VOI voters. The assumption at the time, based on the rollout schedule for the establishment of a worldwide network of Local Registration Authorities, was that many of these voters would have received their certificates by the time the VOI System was operational. In August 1999, the FVAP formally briefed the PKI Working Group session regarding the VOI program requirements and schedule. Still assuming that many volunteers would have received certificates from the PKI PMO, the FVAP requested that a stop-gap procedure be specified for those volunteers who did not yet have their digital certificates. It was decided that these names would be provided to the PKI Working Group and assigned to the nearest issuing authority for processing. As volunteers were added to the VOI Project the FVAP periodically passed their names and locations to the designated PKI point of contact.

To meet project timelines for getting certificates to all the voters in time to participate in the Pilot Project, the FVAP established and executed its own certificate issuing process. The FVAP process entailed issuing[9] and sending documentation for obtaining digital certificates by a commercial carrier or registered mail to the commanding officer of the volunteer voter's unit. This officer was requested to serve as the FVAP's trusted agent to properly identify the recipient and deliver the digital certificate documents. This procedure was further complicated by the fact that these documents expired within 30 days of issue if the digital certificate was not fulfilled. If the recipient was absent from his/her unit when these materials arrived, the documents might be expired by the time he/she received them and the process would have to be repeated. Another difficulty was encountered after citizens received their digital certificates and forgot their passwords. Issuing a new certificate was the only solution for this situation. Of the 157 digital certificates issued to volunteer voters, nearly half (75) had to be replaced. Approximately one-third of these digital certificates were reissued for expired documents; the other two-thirds were reissued because of forgotten passwords.

Assistance to the Voters

The voters were provided a CD-ROM with the required VOI System software and with written documentation on how to install and use the software. A Help Desk was established in January 2000, so that Pilot participants could either speak with a person or leave a message 24 hours a day, 7 days a week. Additionally, the FVAP was in regular contact with VOI voters via e-mail. Pilot participants could also contact the FVAP and their LEO with questions and concerns.

According to the VOI Help Desk logs, 96 percent of the 71 calls logged by the Help Desk were confirmed as resolved. The remaining 4 percent were either questions outside the scope of the pilot (e.g., network problems with the voter's Internet Service Provider) or instances where the Help Desk sent an e-mail with follow-up questions or a proposed solution and the citizen did not reply. Of the 13 calls logged by the Help Desk from the LEOs, 100 percent were resolved.

Figure 1.6-3 illustrates the main problems for which the Help Desk received calls and e-mails. The category, "DoD PKI Digital Certificate Usage" accounted for 34 percent of the Help Desk calls. These calls consisted of a number of PKI-related issues such as participants losing their PKI floppy disks, participants experiencing problems while downloading their certificates, and participants who could not remember their user-specific passwords.

The category, "Access Errors on the VOI Web site," which accounted for 25 percent of all Help Desk calls, represented a variety of problems when citizens could not access the VOI Web site or when they received an error message while completing an action on the site. These errors fall into three categories: citizens who incorrectly typed the VOI Web site address or incorrectly used the site (e.g., citizens did not click on the submit button when required); citizens who received an error message when attempting to perform an action on the VOI Web site; and access control list issues when citizen's names were spelled incorrectly on the access control list.

---

9   Several FVAP personnel were certified as Local Registration Authorities by the PKI program to issue digital certificates.

Twenty-four percent of the Help Desk calls involved issues with the installation of the browser software. These issues ranged from network administrators prohibiting the installation of the software to citizens being unable to complete the installation of Netscape Navigator with the instructions provided.

Figure 1.6-3. Help Desk Calls By Category
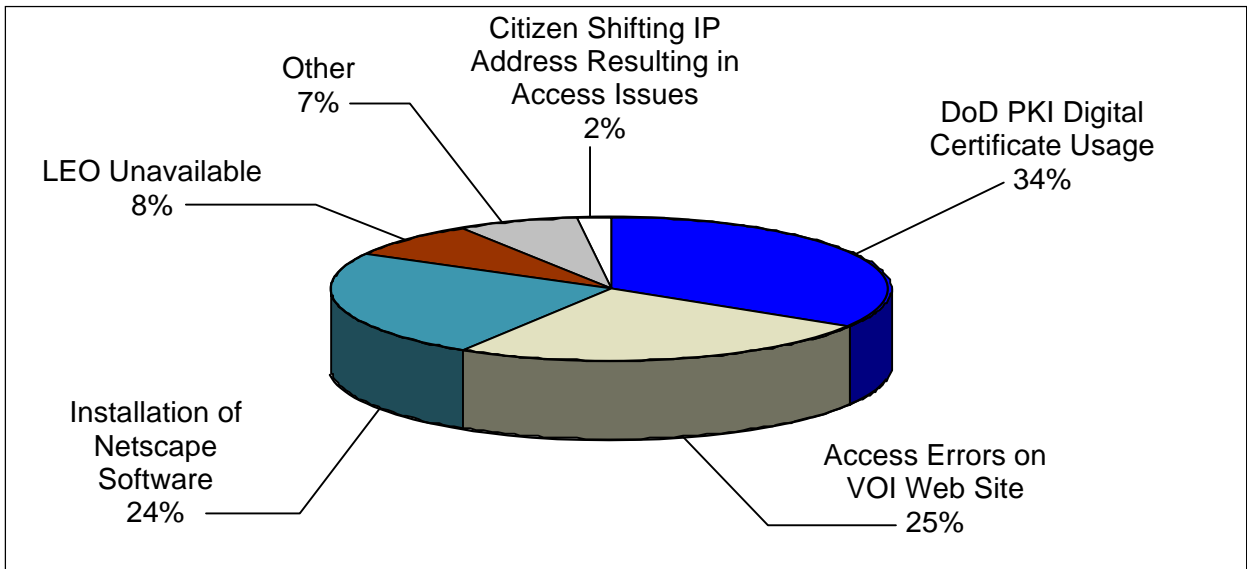
Source: VOI Help Desk Logs

2.0 ASSESSMENT METHODOLOGY

2.1   PURPOSE

The purpose of the assessment was to—

- Assess whether election integrity and a secure and transparent voting process were achieved through the VOI Pilot

- Determine if the VOI Pilot improved *Uniformed and Overseas Citizens Absentee Voting Act* (UOCAVA) citizen access to the absentee voting process

- Consider the implications of scaling the VOI System to support a broader segment of UOCAVA voters

- Provide the Department of Defense (DoD) and the states with information to assist in considering further steps regarding remote Internet registration and voting.

2.2   SCOPE

The assessment team considered whether the VOI Pilot was able to meet the project's objectives of maintaining the integrity of the electoral process, ease of use, and security.[10] The examination also addressed lessons learned and scalability issues that a remote Internet registration and voting system would encounter when implemented on a broader basis.

2.3   METHODOLOGY OVERVIEW

The VOI assessment team chose the hypothesis-driven approach to examine the VOI Pilot Project. The hypotheses provided the framework for the data collection and analysis phase of the examination. This approach allowed the assessment team to—

- Define major components of the VOI Pilot Project to be assessed
- Develop hypothesis statements around these components
- Collect and analyze relevant data
- Draw conclusions based on the best available information and informed judgment
- Prove or disprove the hypothesis statements to identify Pilot issues and findings
- Summarize the issues and findings in a concise format.

2.3.1 Data Collection Tools

The assessment team used various structured interview instruments to collect information from key participants, including the UOCAVA citizens, Local Election Officials (LEOs), Federal Voting Assistance Program (FVAP) personnel, and VOI System developers. Existing documentation including questionnaires, reports, legal code, and technical and administrative documents were also collected.

---

10   Elections must be secure, ensure secrecy of the voted ballots, uphold the integrity of the electoral process, ensure only one vote is counted per voter, and be auditable by election officials.

Comments collected by the Help Desk, e-mail messages, and voter responses to online questionnaires were grouped using content analysis. After all the data were collected, they were aggregated and analyzed.

In addition, the assessment team considered the observations from a workshop of independent experts from the private sector and academia convened by the FVAP to obtain their technical, operational, policy, and legal insights into the VOI Pilot Project. The workshop provided a forum for open, unconstrained dialogue among all the attendees. Project assumptions were questioned, design decisions were explored, and the implications of the limitations of the Pilot were discussed to assist the FVAP in its assessment of the results of the Pilot and its consideration of alternative strategies for any future Internet registration and voting effort.

2.4 LIMITATIONS

This report provides information based on a small population of UOCAVA citizens and LEOs. The data collected highlighted issues and trends, but because of the small size of the Pilot these results cannot be extrapolated to the larger universe of UOCAVA absentee voters.

The following limitations should be kept in mind when reviewing this report—

- The number of participating UOCAVA citizens was a statistically insignificant population size.[11]

- Participants volunteered to be a part of the Pilot versus being randomly selected.

- Nearly all Pilot participants were military members and spouses whose experiences may not accurately reflect those of the broader UOCAVA voting population.

- A very small number of local election offices participated. While the Pilot jurisdictions were quite diverse in their demographics and election administration procedures, they do not constitute a representative cross-section of election offices nationwide.

---

[11] Of the 127 eligible participants that were identified to participate in the VOI Pilot, 91 voters registered and 84 returned voted electronic ballots.

3.0 COMPARISON OF ABSENTEE BY-MAIL AND VOI REGISTRATION AND VOTING PROCESSES

This section provides a comparison of the *Uniformed and Overseas Citizens Absentee Voting Act* (UOCAVA) absentee by-mail registration and voting process and the VOI Pilot System remote absentee registration and voting process.

The VOI System was designed to mirror the UOCAVA absentee by-mail registration and voting process as closely as possible while incorporating new technological capabilities. Participating Local Election Officials (LEOs) followed the same processes and procedures to administer VOI remote registration and voting as they use to administer the UOCAVA absentee by-mail registration and voting. Citizens were encouraged, although not required, to participate in both the absentee by-mail and the VOI processes to ensure that no one would be disenfranchised as a result of a Pilot System malfunction.

Understanding the UOCAVA absentee by-mail and VOI System processes provides the framework for understanding the VOI Pilot assessment, because the findings are based on a comparison of the two processes.

3.1 VOTER REGISTRATION AND ABSENTEE BALLOT REQUEST

UOCAVA Absentee By-Mail Process

To register to vote and request an absentee by-mail ballot, UOCAVA citizens must obtain a Federal Post Card Application (FPCA), complete and affirm the FPCA, and return the FPCA to the appropriate LEO prior to the registration deadline. The FPCA is accepted by all U.S. states and territories as an absentee voter registration application and/or absentee ballot request form. Citizens must accurately complete and sign the FPCA per the state-specific requirements for their voting residences. To complete the FPCA correctly, citizens may need to consult the *Voting Assistance Guide* (VAG) to determine what their state requires. If required, a witness also signs the FPCA to validate the identity of the person submitting the FPCA.

Citizens obtain the FPCA in person or via the postal service or facsimile from a variety of sources including Voting Assistance Officers (VAO), the Federal Voting Assistance Program (FVAP), embassies and consulates, LEOs, and overseas citizens' advocacy groups. If returned to the LEO by the U.S. postal system (including military post offices), the FPCA does not require postage. If the FPCA must be returned via foreign post, sufficient postage must be affixed. The postal service postmarks the FPCA. When there is not sufficient time for delivery of the FPCA through the postal system, the Electronic Transmission Service, administered by the FVAP, provides for the delivery of UOCAVA election materials between LEOs and citizens as allowed by state law. If citizens have any questions about the status of their registration, they may contact the FVAP or the appropriate LEO via telephone, e-mail, or letter to request a status check.

The VOI System

To register to vote and request an absentee ballot using the VOI System, citizens first have to acquire both a DoD PKI digital certificate and the required VOI software. They install the

software on the computer they will use to access the VOI System and download their digital certificates to a floppy disk. Citizens are then ready to access the FVAP server to request an Electronic Federal Post Card Application (EFPCA). The EFPCA is the electronic equivalent of the FPCA; however, the EFPCA is tailored for each LEO site and clearly indicates the information required by each participating state.

To register via the VOI System, the citizen logs on to the FVAP server via the Internet using his/her digital certificate and password and requests an EFPCA by indicating his/her state and/or county of voting residence. Unlike the absentee by-mail process, the citizen does not need to rely on receiving the form from another individual and can log on to the VOI System at his/her convenience. To return the completed EFPCA, the citizen signs it with the digital certificate and password and clicks the submit button. The FVAP server postmarks the EFPCA and forwards it to the appropriate LEO server. The LEO server then issues an immediate message to the citizen acknowledging receipt of the EFPCA. If the citizen has any questions about the status of his/her registration, he/she can access the Check Status feature at any time.

Table 3.1-1 compares the activities associated with voter registration and absentee ballot requests for the by-mail and VOI processes.

Table 3.1-1. Voter Registration and Absentee Ballot Request

ACTIVITY	BY-MAIL PROCESS	VOI SYSTEM
Citizen obtains absentee registration form	• In-person visit to VAO for FPCA • Call/e-mail to FVAP for FPCA	• In-person visit to LRA or trusted agent to get PKI certificate and VOI software • Downloads certificate • Installs software on PC • Accesses FVAP server downloads EFPCA
Citizen completes form	• By hand • Consults VAG for state-specific requirements	• Fills out online EFPCA tailored to state-specific requirements
Citizen affirms completed form	• Signs and dates by hand • Gets witness if required	• Digital signature applied
Citizen returns form to LEO	• Places in mail • Postal Service postmarks	• Clicks on submit button • FVAP server authenticates digital certificate and postmarks • Immediate notice of receipt by LEO server

3.2   LEO PROCESSING OF REGISTRATION REQUEST

UOCAVA Absentee By-Mail Process

The LEO receives the FPCA from a citizen via U.S. mail and identifies and authenticates the citizen by checking the local voter registration database to see if he/she has previously registered to vote. If he/she has, the date and time the FPCA was received are logged into the voter registration database, and the handwritten signature on the FPCA is compared with the signature already on file. If the signatures match and all the required fields on the FPCA are complete and

correct, the citizen's request for an absentee ballot is approved and noted in the database. The LEO also updates the voter registration database with any new information from the FPCA.

If the citizen has not registered with that LEO previously, the FPCA is checked for completeness and address validity. If the form is complete, correct and contains a valid address, the information is logged into the local voter registration database, and the request for an absentee ballot is approved and noted. The citizen is mapped to a specific precinct, which is linked to a particular ballot style. The LEO maintains the FPCA form on file and uses the citizen's signature to compare to future election materials that he/she may submit. The citizen may be sent a voter registration card. If the FPCA is incomplete, a notation in the voter registration database is made and a letter is sent to the citizen to request additional data. If the citizen is found ineligible to vote in the LEO's jurisdiction, a letter is sent to indicate why the application was denied.

The VOI System

To process submitted EFPCAs, the LEO logs on to the LEO server and views the pending EFPCA table. He/she can select an EFPCA to view and uses the information provided to validate the citizen in the same manner used for the absentee by-mail process described above. However, a handwritten signature comparison is not needed because the citizen submits the EFPCA using a digital signature that has already been authenticated by the FVAP server. Because the form cannot be submitted with incomplete data, the LEO only needs to verify that all fields on the EFPCA include correct data. If all the data are valid, the LEO approves the EFPCA, updates the voter registration database, and enters a jurisdiction identifier. If all the data are not valid, the LEO leaves the EFPCA in a pending table and sends an e-mail to the citizen requesting additional information. If the application is denied, the LEO sends an e-mail stating the reason.[12]

Table 3.2-1 compares the activities associated with LEO processing of registration requests for the by-mail and VOI processes.

---

12   E-mail functionality was not a part of the VOI System.

Table 3.2-1. LEO Processing of Registration and Absentee Ballot Request

ACTIVITY	BY-MAIL PROCESS	VOI SYSTEM
Receives registration form	• Sorts FPCAs from mail	• Logs on to LEO administrative workstation, views pending EFPCA table
Verifies data and signature	• Checks voter registration database, other sources • Visually compares signatures	• Checks voter registration database, other sources • Digital signature already authenticated by FVAP server
Requests more information from citizen	• Contacts by mail, e-mail, telephone	• Contacts by e-mail, phone • Places EFPCA in pending status • Citizen can log on to check status
Approves/denies request	• Updates voter registration database and, if approved, maps to a jurisdiction	• Updates voter registration database • Places EFPCA in approved/ disapproved status • Enters a jurisdiction identifier if approved
Notifies citizen of final registration status	• Mails return postcard from FPCA	• Citizen can log on to check status

3.3 ABSENTEE BALLOT PREPARATION, DELIVERY, AND RETURN

UOCAVA Absentee By-Mail Process

After receiving the certified election data to be placed on the ballot from the chief election office, the LEO defines the ballot races and creates the paper ballot using desktop publishing software or other ballot generation tools.[13] The ballot generation database produces the ballot styles for the county and interacts with the voter registration database to automatically map each citizen's jurisdiction identifier to the appropriate ballot style, thereby linking the citizen to the appropriate ballot style. The LEO then manually reviews the ballot styles for correctness and sends the ballot files to the printing company for printing. The printed ballots are returned to the LEO where they are manually checked again.

The LEO mails the blank ballots to the approved citizens. The date the ballots are sent is recorded in the voter registration database. Each citizen receives an absentee ballot via the mail, votes it in secret, inserts the voted ballot into the secrecy envelope and then into the outer mailing envelope. The citizen signs the mailing envelope, and, if required by law, also has a witness sign it. The citizen returns the voted ballot to the appropriate LEO by mail. The postal service postmarks the mailing envelope.

The VOI System

The LEO takes the paper ballots and generates Electronic Ballots (E-Ballots) using the E-Ballot Tool. After creating the E-Ballots, the LEO reviews the HTML files for correctness and then uploads the files to the LEO server. In many instances, the citizen is then informed via e-mail that his/her E-Ballot is ready.

---

13   Ballot generation tools vary from LEO to LEO.

To receive an E-Ballot, the citizen logs on to the FVAP server via the Internet using his/her digital certificate and password, selects the voting residence from the drop-down menu, and requests to vote (i.e., requests a blank E-Ballot). The VOI System logs the date and time the E-Ballot request is made. The citizen receives the E-Ballot, votes it, and submits the encrypted, voted E-Ballot after signing it using the digital certificate and password. The FVAP server "postmarks" the E-Ballot and forwards it to the appropriate LEO server. The LEO server issues an immediate message to the citizen acknowledging that the E-Ballot has been received. If the citizen has any questions about the status of the voted E-Ballot at any time, he/she can access the Check Status feature. The LEOs set their individually determined parameters to specify when to stop providing blank E-Ballots. That date and time are based on the deadline mandated by state election law.

Table 3.3-1 compares the activities associated with absentee ballot preparation, delivery, and return for the by-mail and VOI processes.

Table 3.3-1. Absentee Ballot Preparation, Delivery, and Return

ACTIVITY	BY-MAIL PROCESS	VOI SYSTEM
LEO creates ballots	• Desktop publishing or other software • Jurisdiction identifier automatically mapped to a ballot style	• E-Ballot Tool • Jurisdiction identifier manually mapped to a ballot style
Ballots reviewed	• Manual review of paper ballots	• Manual review of HTML files
Ballots produced	• Sends ballot files to printer • Printer delivers paper ballots to LEO	• Uploads E-Ballot files to LEO server
Pre-mail ballot review	• Manual review of paper ballot	• No additional review steps required
Ballot delivered	• Labels prepared, envelopes stuffed, placed in mail, date logged	• E-Ballot delivered on demand to citizen
Citizen receives ballot	• Retrieves from mailbox	• Downloads E-Ballot • System automatically logs date and time
Citizen votes ballot	• Marks paper ballot by hand	• Clicks E-Ballot choices with mouse and keyboard
Citizen secures voted ballot	• Seals paper ballot in privacy envelope, then places in mailing envelope	• Clicks submit button and encrypts ballot
Citizen signs/dates mailing envelope and oath	• By hand • Gets witness if required	• Applies digital signature
Citizen returns ballot to LEO	• Places in mail • Postal Service postmarks	• Encrypted E-Ballot transmitted • FVAP server authenticates digital certificate and "postmarks" • Immediate notice to citizen of receipt by LEO server

3.4 BALLOT RECONCILIATION, PROCESSING, AND TABULATION

UOCAVA Absentee By-Mail Process

The date and time the voted absentee by-mail ballot is received at the LEO is recorded in the voter registration database. The LEO checks the validity of the outer absentee envelope to ensure that all data requirements are met, including the postmark, citizen signature, and witness information if required. The LEO then authenticates the voter's identity by comparing the signature on the mailing envelope with the signature on file. If the data are complete and the signatures match, the ballot is grouped with other valid ballots and stored securely until time to process. If the data are not complete or the signatures do not match, the ballot is stamped invalid and then placed with other invalid ballots for auditing purposes.

At the specified processing time, the LEO removes the secrecy envelopes from the mailing envelopes, randomizes the order by mixing them, and then removes the voted ballots from the secrecy envelopes. At this time all ballots are anonymous unless the voter has made a distinguishing mark on the ballot that would identify him/her. Any marked or damaged ballots are manually transcribed to replacement ballots, noted as "replacement" or "duplicate" and placed with the valid ballots. The valid ballots are then placed in the tabulation system and the votes counted.

The VOI System

To process E-Ballots, the LEO logs on to the LEO server and views the Ballot Reconciliation Table, reconciles the E-Ballots and validates them using the same criteria as the by-mail process. If any ballots are invalidated, the LEO can enter a reason. A handwritten signature comparison does not need to be performed because the citizen has already been authenticated by the FVAP server. The encrypted E-Ballots remain stored in the LEO server database.

At the appropriate time, the LEO selects all the E-Ballot types to be processed and invokes the manual procedure required to start the E-Ballot decryption process. The first step is to have the two designated LEO staff with the privacy key floppy disk and the privacy key password insert the floppy disk and enter the password into the LEO server. Then the LEO clicks the Final E-Ballot Processing button. The LEO server separates the citizens' identification from the encrypted voted E-Ballots, decrypts the E-Ballots, and randomizes and prints them. If there is a printer malfunction, the LEO can selectively reprint anonymous ballots individually, by ballot style, or all.

The contents of the printed E-Ballots are transcribed on to blank absentee ballots that can be tabulated by the same tool used to tabulate by-mail voted ballots. The E-Ballot printed from the VOI System is marked invalid, and the replacement ballot is marked "replacement" or "duplicate" and placed with the other valid absentee by-mail voted ballots. All the transcribed ballots are grouped with the by-mail ballots and tabulated.

Table 3.4-1 compares the activities associated with ballot reconciliation and tabulation for the by-mail and VOI processes.

Table 3.4-1. Ballot Reconciliation, Processing, and Tabulation

ACTIVITY	BY-MAIL PROCESS	VOI SYSTEM
LEO reconciles absentee ballots	• Visually verifies signature against file copy • Performs other validation checks	• Views E-Ballot table at administrative workstation • Signature already authenticated by FVAP server • Performs other validation checks
Ballots stored for processing at prescribed time	• Valid ballots are placed in the ballot box • Invalid ballots stored separately	• Marks E-Ballots valid or invalid in reconciliation table • All E-Ballots remain stored in database in encrypted form
Ballots prepared for tabulation	• Opens ballot box • Removes mailing envelopes • Randomizes order • Removes secrecy envelopes	• Two LEO personnel insert privacy key and enter password on LEO server • System selects valid E-Ballots, removes signatures, decrypts, randomizes, and prints E-Ballots in continuous automated process
Ballots tabulated	• Paper ballots placed in tabulating system	• Printed E-Ballots manually transcribed to paper ballots • Ballots placed in tabulating system

3.5 COMPARISON SUMMARY

Although the VOI processes and procedures were designed to mirror the UOCAVA absentee by-mail processes, several differences in the implementation of the VOI System existed. In the absentee by-mail process, citizens received their FPCAs from their VAOs, the FVAP, and LEOs. During the VOI Pilot, citizens did not need to rely on the VAOs for forms but instead logged on to the FVAP server at their convenience and requested the EFPCAs. In the UOCAVA absentee by-mail process, LEOs mail the ballots to citizens as soon as they are available. In the VOI System, citizens logged on to the system to request their ballots from the LEO.

In the by-mail process, the citizens have to contact the LEO or FVAP if they want information about the status of their registration requests or ballot availability. In the VOI process, citizens can get this information by logging on to the system.

In the absentee by-mail process, LEOs perform a manual signature verification process to authenticate the voter. Through the VOI System, the LEOs no longer perform the signature or witness verification process. The VOI participants were given digital certificates and Local Registration Authorities or trusted agents authenticated their identities when the digital certificates were distributed. The FVAP server then authenticated the citizen's identity by validating his/her digital certificate.

4.0 ASSESSMENT FINDINGS

This section presents the key Voting Over the Internet (VOI) Pilot assessment findings. This discussion addresses the three major questions relative to the VOI Pilot Project—

- Did the Pilot maintain the integrity of the electoral process?

- Did the Pilot enhance the enfranchisement of UOCAVA citizens?

- What new issues and risks does the technology introduce?

When reviewing these findings, it is important to bear in mind that they are based on a very small project with limited scope and objectives. The UOCAVA population experiences difficulties in exercising their right to vote which are not shared by the U.S. voting population at large. The participating local election offices (LEOs) and voters were all volunteers; therefore, one could assume that they might be more favorably disposed toward the use of technology than the "average" citizen or election official. Nearly all the voters were Service members or spouses whose circumstances differ significantly from civilian UOCAVA voters. Every aspect of the project was closely controlled and the technical elements were under the constant oversight of a highly skilled team of engineers. The VOI System was designed and operated as a dedicated, stand-alone system with no automated interfaces to existing election administration systems. This resulted in some duplication of effort and adaptation of normal LEO procedures during the Pilot.

In summary, these findings should be taken as preliminary indicators of the feasibility of remote Internet voting, applicable to a special population group. There is still a considerable amount to be learned about the use of this technology and how well it can be integrated into the absentee registration and voting process.

4.1 THE VOI SYSTEM MAINTAINED THE INTEGRITY OF THE ELECTORAL PROCESS

All voting systems must maintain the integrity of the electoral process. The integrity of the electoral process is the foundation on which the legitimacy of election results is based. The electoral process begins with the qualification and registration of citizens to vote and, in the usual case, concludes with the canvassing of ballots following an election. To maintain the integrity of this process, the VOI System had to reliably identify and authenticate registrants, limit voting to only registered persons, ensure that not more than one ballot would be counted for each registered voter, prevent alteration of the unvoted and voted ballots, protect the ballots during transit, provide secrecy of the ballot, create a documentation trail for auditing and recount purposes, and comply with all legal requirements.

Many argue that a remote Internet registration and voting system cannot provide electoral process integrity. However, every voting system has levels of risk. The current UOCAVA absentee by-mail registration and voting process has a certain level of risk that is considered outweighed by the benefit of enabling this group of citizens to vote. The relevant questions are whether the VOI Pilot provided more benefits to the UOCAVA citizens and the LEOs with the

same or fewer risks than the current UOCAVA absentee by-mail registration and voting process, and whether the risks to the integrity of the electoral process posed by the VOI Pilot were acceptable in light of these benefits.

The VOI Pilot maintained the integrity of the electoral process, and in many respects posed fewer risks to election integrity than the current UOCAVA absentee by-mail process. Specifically, the VOI Pilot—

- Identified and authenticated VOI Pilot registrants with a high degree of confidence

- Limited voting to only identified and authenticated VOI Pilot registrants

- Ensured that not more than one electronic ballot (E-Ballot) was submitted by each VOI Pilot voter

- Ensured that only one ballot was counted for each VOI Pilot voter

- Provided greater protection against the alteration of ballots than the UOCAVA absentee by-mail process

- Successfully protected E-Ballots while in transit between the LEO servers and VOI Pilot participants

- Provided secrecy of the ballot

- Facilitated post-election audits and recounts

- Complied with all legal requirements of the participating jurisdictions.

The following sub-sections discuss each of these elements of electoral integrity. For each element, the sub-section describes why that element is important, summarizes how the UOCAVA absentee by-mail process addressed that element, and describes how the VOI System maintained that element of integrity.

4.1.1 The VOI System Identified and Authenticated VOI Pilot Participants With a Higher Degree of Confidence Than the UOCAVA By-Mail Process

In the case of the VOI Pilot, identification refers to the System's ability to correctly identify who is sending and receiving election materials. Authentication refers to the System's ability to verify the person sending the election materials is the person he/she claims to be. To confirm that only eligible persons vote in an election, it is imperative that election officials have an effective means of identifying and authenticating persons registering to vote in a particular county from remote locations.

The UOCAVA Absentee By-Mail Process

In the UOCAVA absentee by-mail process, the registration applicant does not appear in person to register nor does the applicant need to provide identification to register. If the citizen is registering in the county for the first time, the LEO identifies and authenticates the voter by validating the address and other information provided by the registrant on the Federal Post Card

Application (FPCA). If the applicant has registered previously, the LEO compares the signature on the FPCA with the signature on file to identify that the same person submitted the FPCA.

The VOI System

The VOI Pilot identified and authenticated registrants with a higher level of assurance than the absentee by-mail process. This was accomplished through the use of digital certificates, an access control list, and manual processes completed by the LEOs. When qualified to participate in the Pilot, the citizen was required to receive a DoD Medium Assurance PKI digital certificate before he/she could access the System. This required a personal appearance before a Local Registration Authority or trusted agent with official photo identification.

An additional method the VOI System used to identify and authenticate valid VOI users was an access control list. The access control list limited VOI System access to authorized users who were entered into a database. Some users initially could not access the System because their names were not yet entered or had been misspelled. This problem, which was quickly resolved, demonstrated that the list successfully prevented access by unauthorized users.

A review of the FVAP server logs after the System was shut down indicated that only successfully identified and authenticated users who had the appropriate digital certificates and passwords for the System were given access.

4.1.2 The VOI Pilot Successfully Limited Voting to Identified and Authenticated Registrants

To ensure that only eligible UOCAVA citizens vote, a remote voting system must ensure that only properly registered citizens vote.

The UOCAVA Absentee By-Mail Process

The UOCAVA absentee by-mail process limits voting to registered citizens through several means. First, only registered citizens are mailed an absentee ballot. Second, UOCAVA voters are sometimes required to have their signatures on the mailing envelope witnessed or notarized. This process helps ensure the person voting the ballot is indeed the registered voter. Third, the LEOs compare the signature on each UOCAVA mailing envelope with the voter's signature on file to ensure they match.

The VOI System

The VOI System provided an extremely high level of confidence that all VOI Pilot voters were registered to vote using the System. When a voter requested an E-Ballot, the System would check if his/her name appeared in the approved Electronic Federal Post Card Application (EFPCA) table and if a valid ballot type had been assigned. In order for his/her name to be in this table, the LEO had to take an action to review and approve the EFPCA and thereby move the application from the pending table. The LEO would manually enter the ballot type assignment after obtaining this information from the voter registration database (not a VOI System component). A review of FVAP server log data showed that no E-Ballots were distributed to citizens whose EFPCAs had not been approved.

4.1.3 The VOI System Ensured That Only One Voted E-Ballot Was Submitted for Each VOI Pilot Voter

The UOCAVA Absentee By-Mail Process

In the by-mail process, the LEO sends only one absentee ballot to each eligible voter. The ballot style and mailing date are noted in the voter's record. Should the paper ballot get damaged in transit, the citizen can request a replacement ballot if time allows. The damaged ballot must be returned with the request.

The VOI System

The VOI System used an automated method to ensure that VOI participants could not submit more than one voted E-Ballot. After the LEO server received a voted E-Ballot from a citizen, the system was programmed to deny any further requests by the same user to download another blank E-Ballot.

The FVAP and LEO server log data confirmed that VOI participants did not submit more than one voted E-Ballot. After returning a voted E-Ballot, four VOI participants requested another blank E-Ballot. The VOI System denied each request.

4.1.4 The VOI System Ensured That Only One Ballot Was Counted for Each VOI Pilot Voter

To maintain election integrity, a voting system must make certain that not more than one ballot is counted for each registered voter.

The UOCAVA Absentee By-Mail Process

In the by-mail process, the LEOs perform a reconciliation function to determine if more than one absentee ballot was received from any voter, or if a voter voted in person at the polls and also submitted an absentee ballot. A voter could legitimately return more than one absentee ballot in those jurisdictions (such as Florida) that provide advance ballots as well as regular absentee ballots. The voter also might have returned a Federal Write-In Absentee Ballot if he/she thought the requested state absentee ballot would not arrive in time. Each LEO has an established procedure and criteria to determine which ballot gets counted when more than one ballot is received from a single voter.

The VOI System

As previously discussed, the VOI voters were asked to submit a paper by-mail ballot as a backup procedure. In order to count the E-Ballots rather than these backup ballots, the LEOs established a procedure to identify and hold aside any by-mail ballots received from VOI voters until the close of polls. At that time they would perform the usual ballot reconciliation process to determine if more than one ballot was received from any voter. If they received an E-Ballot and a paper ballot they would mark the paper ballot duplicate, set it aside and count the E-Ballot. However, ten paper ballots from VOI voters were inadvertently placed in ballot boxes. Once a ballot has been placed in the ballot box, it cannot be removed; so these ten paper ballots were

counted. When reconciling the E-Ballots, the LEO invalidated the ones from these ten voters, ensuring that only one ballot was counted for each voter.

4.1.5 The VOI System Provided Greater Protection Against the Alteration of Ballots Than the UOCAVA Absentee By-Mail Process

To maintain the integrity of an election, ballots must be protected from alteration while in the possession of the LEO or the voter and during transit.

The UOCAVA Absentee By-Mail Process

LEOs provide physical security to protect voted ballots received via the UOCAVA absentee by-mail process. After the signature is validated on the mailing envelope, the absentee by-mail ballot is deposited in a sealed ballot box. LEO personnel with access to ballot boxes are trained, trustworthy, and supervised. Although physical alteration of the paper ballot is possible, it is difficult to conceal unless the ballot is copied as a new document. While the ballot is in the voter's possession, it is his/her responsibility to maintain its security.

In the UOCAVA absentee by-mail process, the voter places his/her ballot in a secrecy envelope and then in an outer mailing envelope for transit. These ballots are protected by the standard security measures of the domestic and/or foreign postal systems.

The VOI System

Because there is no physical document to verify in an electronic voting system, safeguards must be put in place to ensure E-Ballots are not tampered with.

The VOI System provided superior protection against the alteration of E-Ballots. It prevented intruders from accessing the VOI E-Ballots through the use of—

- Encryption and digital signatures
- Secure operating system configuration
- Intrusion detection systems
- Communication routers with access control filters.

- Encryption and Digital Signatures

To protect against E-Ballot alteration, the VOI System employed encryption and digital signatures. Voted E-Ballots were encrypted before transmission to the LEO server to maintain the secrecy of the E-Ballot. Once at the LEO server, the voted E-Ballots were also stored on the LEO server in their encrypted states until the LEO was ready to process them. If an intruder had been able to access an E-Ballot, he/she would not have been able to read it because the contents were encrypted. Transmissions across the Internet were also encrypted using Secure Sockets Layer (SSL) technology, a Web standard that is considered very secure.

In addition to encryption, digital signatures were used to maintain the integrity of election materials transmitted via the VOI System. Citizens used their digital certificates to sign their election materials so LEOs would be able to verify that the citizen sending the material was in

fact the person he/she claimed to be. The LEO used an identity digital certificate to verify his/her identity to the System and a commercially provided privacy digital certificate to maintain the secrecy of the voted E-Ballot. In the unlikely event that an intruder had defeated the encryption and altered an E-Ballot, the VOI System would have detected the alteration because the hash code associated with the digital signature would not have matched the original hash created when the election materials were digitally signed.

For further protection, LEOs maintained two-person control of the private key of the privacy certificate. Because one official knew the password and the other official had physical control of the digital certificate, one official could not decrypt ballots without the interaction of the other official.

- Secure Operating System Configuration

Windows NT must be configured properly to ensure server security. System testers attempted to access the VOI System through such protocols as Secure Hypertext Transfer Protocol, File Transfer Protocol, and Simple Mail Transfer Protocol. Testing showed that the VOI System successfully prevented 100 percent of access attempts as a result of proper configuration. This secure configuration helped prevent ballot alteration by preventing unauthorized access to the server.

- Intrusion Detection Systems

The FVAP server segment had two intrusion detection systems that monitored for unauthorized access to the VOI System. The first one, located inside the router, would have alerted administrators to attempted breaches of the System that were not thwarted by the access control filters on the router. The second, located outside the router, was used to alert administrators to probes and other activities that could forecast an attempt on the System. Probing was detected (some of which was attributed to intentional testing), but no follow-on intrusion attempts were detected. The VOI System kept detailed logs that could be reviewed to detect unusual events that might have signaled an attempted or actual security breach.

- Communication Routers with Access Control Filters

All communications between the citizens and the LEO servers flowed through the router located within the FVAP server segment architecture and at each LEO site. All routers were equipped with access control filters that managed traffic between the servers. The access control filters allowed the VOI System to restrict the flow of data based on its origination, destination, or the type of low level communication protocol used. This capability added a significant layer of security to the VOI System. For example, the fixed Internet addresses of the FVAP and LEO servers allowed them to identify each other. This direct communication was enforced by the routers at both ends. In addition, the LEO servers and routers were physically secured within locked rooms in secure, restricted access areas to deter tampering. If the LEO router settings were changed, the FVAP system check would identify the LEO server as non-operational.

The VOI System passed 100 percent of all security tests performed to verify the reliability of the end-to-end encryption scheme.

4.1.6 The VOI System Successfully Provided Secrecy of the Ballot

Secrecy of the ballot means that no one can connect a voter's identity with the contents of his/her ballot. Secrecy helps facilitate freedom of choice by discouraging direct and indirect coercion in voter selections.

The UOCAVA Absentee By-Mail Process

With absentee by-mail voting, secrecy is maintained through the voter placing the voted ballot in a secrecy envelope that contains no identifying information. The secrecy envelope is inserted into a mailing envelope and sent to the LEO. When it is time to process the absentee ballots, election workers remove the secrecy envelopes from the outer mailing envelopes. The now anonymous ballots are randomized, the secrecy envelopes removed, and the ballots counted.

There is one circumstance in which the absentee voter's identity could possibly be linked with his/her absentee ballot. This is when only one absentee voter receives a particular ballot style in a precinct. An election worker could check the records to see who received this ballot style and thus connect the voter's identity to his/her vote. Furthermore, all jurisdictions publish voting results by precinct, and some also publish lists of those who voted absentee by precinct. Therefore, it could be possible for someone in the public to match up the voter with his/her vote in this unusual situation.

The VOI System

The VOI System preserved the secrecy of the E-Ballot using several techniques.

As discussed above, the voted E-Ballot was encrypted first by the VOI plug-in and again during transit using SSL. Because the voted E-Ballot was encrypted, the voter's choices were protected from observation. Although it is possible to defeat encryption, the level of effort and skill required makes the process prohibitively expensive and time consuming.

To maintain the secrecy of voted ballots, the LEO server separated the digital signatures from the voted E-Ballots before they were decrypted and printed. The ballot processing software on the LEO server randomized the ballots after the signatures were removed and before they were printed, so that a printed E-Ballot could not be linked by order to a voter. This process provided a high level of secrecy protection for VOI Pilot voters.

Independent testing showed the VOI System passed 100 percent of the transmission confidentiality tests. Testing also showed that in all cases, E-Ballot processing removed the links between voter identity and the E-Ballot choices, maintaining the secrecy of the ballot.

As is true in the by-mail process, if only one VOI Pilot voter received a particular E-Ballot style, the voter's E-Ballot could be linked to the voter in the same manner by checking the records to see who was assigned this E-Ballot style. It was recognized in the course of the Pilot that the probability of this happening was fairly high because of the small number of participating voters. This was a particular concern in South Carolina where several counties had only one VOI volunteer. As a result, the South Carolina volunteers were advised of this possibility and all

chose to continue their participation. In a full-scale Internet voting system with a large number of voters, this situation would be far less likely to occur.

4.1.7 The VOI System Facilitated Post-Election Audits and Recounts

The success of a democracy rests in part on the public's confidence in the process used to elect public officials. Although all citizens may not champion the winner, all must be confident the final choice reflects the will of the people. To garner such confidence, measures must be in place to re-create the election should the legitimacy of the outcome be in doubt. For this reason, LEOs maintain detailed documentation trails recording specific election events to facilitate post-election audits and, if necessary, partial or total vote recounts.

The UOCAVA Absentee By-Mail Process

In the UOCAVA absentee by-mail process, LEOs maintain a documentation trail recording specific election events through a combination of hard copy files and computerized records. This documentation trail notes such activities as the date absentee ballots were mailed, the names of the recipients of absentee ballots, and the date the voted absentee ballots were returned to the LEO. If a recount becomes necessary, the paper ballots can be made available for recounting.

One challenge for LEOs is the inherent conflict between the need for auditability and the need to preserve voted ballot secrecy. In the UOCAVA by-mail process, the balance is struck by using the anonymous secrecy envelope and the mailing envelope that identifies the voter. The outer mailing envelope identifies the voter for record keeping and auditing purposes, and the inner privacy envelope guards the secrecy of the voter's selections when the mailing envelope is removed.

The VOI System

The VOI System was designed to maintain detailed transaction logs of System events to facilitate post-election audits and recounts. For example, VOI System transaction and security logs recorded all citizen log-ins, all EFPCA or E-Ballot requests and submissions, all Status Check requests, all denied requests for materials, and all instances in which the LEO server was not responding. The logs could be queried by different variables, such as the user common name, which allowed administrators to review the activities of a specific VOI user or time period. The system administrators could then reconstruct activities during a given period of time.

Independent testers of the VOI System examined the logging feature on the FVAP and LEO servers. They found that both servers were successful in logging and storing all transactions performed on the VOI System, from the time the citizen first logged on and requested an E-Ballot to the end of the process when the E-Ballots were received and printed. These tests showed that the FVAP servers met 100 percent of their requirements for the maintenance and accessibility of transaction logs.

The VOI System also assigned printer control numbers to the printed E-Ballots, which allowed the LEOs to determine if certain E-Ballots needed to be reprinted as a result of a printing error, printer jam, or unreadable printout. A similar identifier is used on paper ballots to facilitate the recount process.

For partial and total recount purposes, the LEOs were able to reprint processed E-Ballots by printer control number, E-Ballot type, or all the E-Ballots. In the event that the LEO wished to carry out a total recount with unprocessed E-Ballots due to a challenged election, the LEO could use the "reset E-Ballot processing" feature. This feature allowed the LEOs to reset all E-Ballot reconciliation and E-Ballot processing to its original state after the voted E-Ballots were received from the citizens. This activity placed all the voted E-Ballots back into the reconciliation table marked as unprocessed. The LEO could then re-reconcile and re-process all the voted, encrypted E-Ballots and reprint them in random order. Independent testing determined that the System passed all functional tests pertaining to this capability.

4.1.8 The VOI System Complied With All Legal Requirements in the Participating Jurisdictions

The United States Constitution reserves to the states the authority to determine the time, place, and manner of holding elections. Accordingly, each state has its own legislation and regulations setting forth registration and voting requirements and procedures. Although many similarities exist among state election laws, there are distinct requirements and procedures in each state.

The VOI System developers faced the significant challenge of developing a remote registration and voting mechanism that would comply with both Federal law and the state law in each Pilot jurisdiction. To a large extent, the designers relied on, and were greatly assisted by, the election officials in each VOI Pilot state and county to ensure that all legal requirements were identified. Election officials and the VOI System developers also worked together to ensure the VOI System contained sufficient features to meet the variety of state laws addressing, for example, ballot design and oath statements.

4.1.9 The Design of the VOI System Enabled Remote Registration and Voting in Compliance With All Federal and State Voting Requirements for the Participating VOI Pilot Sites

Federal Law Relevant to UOCAVA Absentee Registration and Voting

> *- Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)*

The federal law that protects absentee registration and voting by the Uniformed Services and overseas citizens is the *Uniformed and Overseas Citizens Absentee Voting Act* (42 U.S.C. § 1973ff). This law permits members of the Uniformed Services, merchant marine, their eligible family members, and U.S. citizens residing outside the United States to register and vote absentee in federal elections. The VOI Pilot complied with, and directly promoted, the overall and specific goals of the UOCAVA.

> *- Section 5 of the Voting Rights Act*

Section 5 of the Voting Rights Act (42 U.S.C. § 1973c) freezes changes in election practices or procedures in certain states until the new procedures have been "precleared" through administrative review by the United States Attorney General. This means that voting changes in covered jurisdictions may not be used until Section 5 preclearance has been obtained. Section 5

preclearance will be denied if the proposed change has not been shown to be free of the purpose and the effect of discriminating on the basis of race or membership in a language minority group.

The State of South Carolina and Dallas County, Texas, were required to request preclearance of the use of the VOI Pilot System. The South Carolina legislature passed special legislation (Act R.423, 1998) allowing for the implementation of the Pilot Project in that state. This legislation was submitted to the Voting Section of the Civil Rights Division in June 1998 for preclearance review. The U.S. Department of Justice made a determination of no objection to the proposed changes and gave its approval in August 1998. Dallas County, Texas, submitted their preclearance request in November 2000 which was approved the same month through expedited consideration by the Department of Justice.

- Sections 203 and 4(f)(4) of the Voting Rights Act

The language minority provisions of the Voting Rights Act are codified at § 203 (42 U.S.C. § 1973 aa-la) and § 4(f)(4) (42 U.S.C. § 1973 4(f)(4)). These provisions require certain covered jurisdictions to provide bilingual written materials and other assistance. Dallas County, Texas, was required to submit a sample of its bilingual (English and Spanish) E-Ballot to comply with this provision. This sample was provided with the Section 5 preclearance request to the Department of Justice and approved in November 2000.

The VOI Pilot Complied With All Relevant State Legal Requirements in the Participating Jurisdictions

As stated above, each state has its own election laws and regulations. However, a number of common requirements exist in the statutory scheme of each Pilot state. These requirements include—

- Use of an approved registration form
- Certification or approval of voting equipment or systems
- Ballot design requirements
- Oath requirements
- Signature and witnessing requirements for both registration forms and absentee ballots
- Deadlines for submission of registration forms/ballot applications and voted ballots.

A careful analysis of the election laws in each Pilot state demonstrated that the VOI Pilot complied with all relevant legal requirements. This section addresses the VOI System's compliance, generally, with the basic state law requirements listed above.

Each Pilot state requires absentee registrants to register to vote and/or request a ballot using a designated form. The VOI Pilot complied with these requirements in each Pilot state. The laws of Florida, South Carolina, Texas, and Utah allow Uniformed Services and overseas voters to register and/or request ballots using the FPCA. The VOI Pilot complied with these requirements because each VOI Pilot registrant used an electronic version of the FPCA.

Each Pilot jurisdiction has a law or laws requiring voting systems to be—

- Certified by election officials
- Approved by election officials
- Compliant with technical standards for voting equipment or systems.

The VOI Pilot complied with all state certification and approval requirements for voting equipment or systems. In Florida, the state issued a formal certification to the VOI System pursuant to Florida law. In the other Pilot jurisdictions, election officials determined that Florida's certification was sufficient to demonstrate that the VOI System also met the certification requirements in their states. In addition, the VOI Pilot complied with all technical requirements generally applicable to voting equipment or systems in each Pilot state.

Each Pilot state has legislation requiring several specific ballot design features. The VOI Pilot met all state requirements regarding ballot design. For example, some Pilot states allow voters to write in the name of a candidate not listed on the ballot. Some of the LEOs are required to provide ballots in English and Spanish. Ballot instructions may also vary by LEO. The VOI System met these design requirements because of the E-Ballot Tool's ability to customize E-Ballots.

Each Pilot state requires each absentee voter to swear an oath. The oath set forth on the FPCA has been approved by all states. The VOI System's EFPCA contained the identical oath and required the registrant to swear or affirm this oath. In addition, the E-Ballots for each jurisdiction contained the text of the oath required by that state. The voter was required to check a box indicating his/her swearing or affirming that oath. Accordingly, the VOI Pilot met all state oath requirements.

Each Pilot state requires an absentee voter to sign the registration form and the ballot return envelope. Some, but not all, Pilot states require the signature to be witnessed for the purpose of authenticating the voter's identity. The use of DoD Medium Assurance PKI digital certificates in the VOI Pilot fulfilled this function and was consistent with laws in each Pilot state regarding electronic and/or digital signatures. The VOI Pilot met all signature and witnessing requirements.

Each Pilot jurisdiction has deadlines for submitting the FPCA and submitting a voted absentee ballot. The deadlines vary somewhat from state to state. Each LEO could set parameters on the LEO server to reflect the particular time periods for the state. Several registrants submitted their EFPCAs after the registration/ballot request deadline. In each case, the registrant was allowed to vote if he/she had also submitted a paper FPCA by the deadline. In two instances where late VOI registrants had not submitted a paper FPCA, the citizens were not allowed to vote.

With one exception, all E-Ballots were requested and submitted by the prescribed deadlines. The exception occurred in South Carolina, which has a cutoff of 5:00 p.m. the day before the election for absentee ballot requests. One South Carolina voter requested an E-Ballot on election day. Since the instructions in the citizen information packet did not reflect this pre-election day cut-off, the South Carolina officials waived the deadline, and the citizen was allowed to download the E-Ballot.

4.2 THE VOI SYSTEM ENHANCED THE ENFRANCHISEMENT OF UOCAVA CITIZENS AND ADDRESSED BY-MAIL REGISTRATION AND VOTING CHALLENGES

The VOI System was developed to provide an alternative method of voting that not only alleviates some of the traditional barriers to participation in an election experienced by UOCAVA citizens, but also eases the burden placed on the LEOs.

The by-mail challenges in UOCAVA absentee registration and voting addressed by the VOI System include—

- Submission of incomplete or incorrect documentation
- Mail transit time
- Availability of election materials
- Mobility of UOCAVA citizens
- Obtaining information on the election process
- Burden of administering elections for remote voters.

The following sub-sections summarize the issues and then discuss how the VOI System mitigated the problems.

4.2.1 VOI Significantly Reduced UOCAVA Absentee By-Mail Registration and Voting Problems Arising From Inaccurate, Incomplete, or Unclear Data

The UOCAVA Absentee By-Mail Process

According to election officials, many UOCAVA citizens are prevented from participating or having their votes counted in an election due to incomplete, inaccurate, or unclear information on the FPCA and/or the absentee voted ballot. For instance, a significant number of FPCAs received by LEOs are incomplete or illegible. Common types of missing or incomplete information include the legal voting address, current mailing address, signature, witness signature, and witness address. In those instances where the form is incomplete but legible, the LEO contacts the applicant to request additional information. Although some voters return the necessary information, many do not, and their FPCAs cannot be approved, thus preventing them from receiving absentee ballots.

As illustrated in Figure 4.2-1, the FVAP Fifteenth Report, using data from the 1996 FVAP Post Election Survey Final Report, ranks common problems LEOs experience when processing FPCAs.

Similar problems also occur with the processing of UOCAVA absentee ballots. Based on data provided by the LEOs from the VOI Pilot jurisdictions, the most common reasons for invalidating UOCAVA absentee by-mail voted ballots in the 2000 General Election are no citizen signature, nonmatching signatures, and no witness signature/address. The data are presented in Figure 4.2-2.

In addition, many UOCAVA ballots are invalidated because of postmark issues. In some states, UOCAVA absentee by-mail voted ballots must have a military or foreign postmark to be counted

after the close of polls. As demonstrated in Florida in the 2000 General Election and noted during VOI LEO interviews, some UOCAVA ballots arrived without valid postmarks.

UOCAVA ballots are sometimes returned to the wrong LEO and may be excluded from tabulation if there is not enough time to forward the ballot to the correct LEO. Portions of ballots may be excluded from tabulation if the mark made by the citizen is unclear and the intent of the voter is not apparent. Data received from three of the counties participating in the VOI Pilot indicated that the percentage of the by-mail UOCAVA ballots invalidated (attributed to a number of reasons) ranged from 1 percent to 11 percent.

Figure 4.2-1. Ranking of Problems Experienced in Processing FPCAs by Local Election Officials for the 1996 General Election
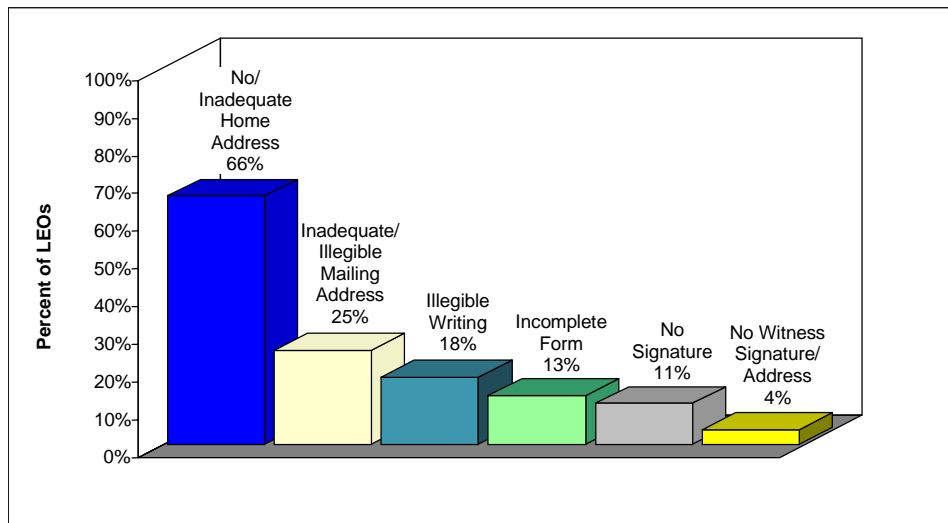
Source: The FVAP Fifteenth Report, December 1997

Figure 4.2-2. Reasons for Invalidating Voted By-Mail Ballots in the 2000 General Election, in the Five VOI Jurisdictions
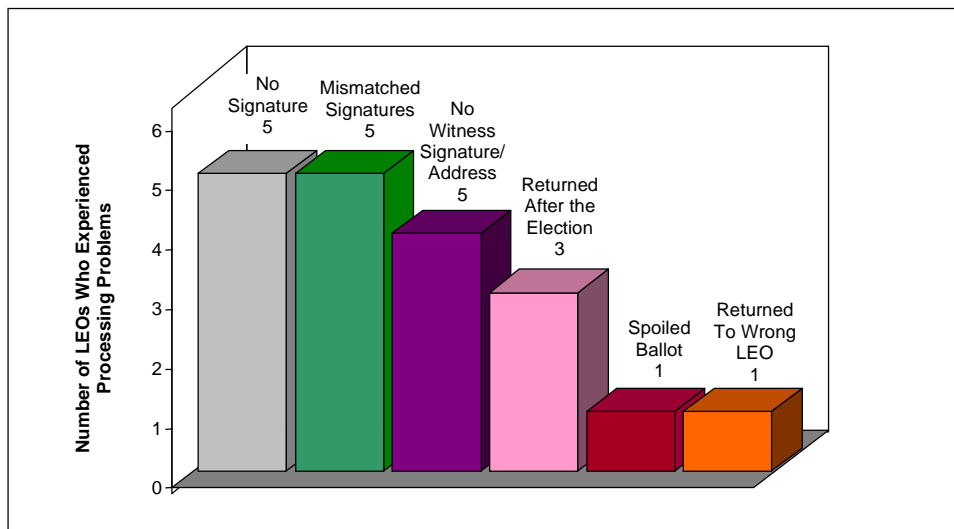
Source: 2000 LEO Participating Data

The VOI System

The VOI System eliminated incomplete and illegible registration applications through several System features, as outlined in Table 4.2-1. The VOI System prompted users to complete all required fields in the EFPCA before submitting the form. Keystroking of information took the place of handwriting. Finally, the EFPCA could not be submitted without the use of a DoD PKI digital certificate, which served as the citizen's signature and replaced the need for a witness or notary signature.

**Table 4.2-1. How the VOI System's EFPCA Design Features
Addressed FPCA Processing Problems**

FPCA PROCESSING PROBLEMS	VOI SYSTEM EFPCA DESIGN FEATURES
No/inadequate voting address	• Through online reminders, citizens are prompted to complete all required fields
Inadequate/illegible mailing address	• There is increased data legibility through keystroked text
Illegible writing	• There is increased data legibility through keystroked text
Incomplete form	• Through online reminders, citizens are prompted to complete all required fields
No citizen signature	• The digital signature serves as citizen signature
No witness signature/address	• The digital signature replaces the need for a witness

The VOI System design also eliminated the possibility of submitting an unclear or incomplete absentee voted ballot through several VOI System features as outlined in Table 4.2-2. The VOI System provided the "postmark" in place of the post office and substituted digital signatures for the citizen and witness signatures. In addition, online prompts alerted the citizen to the fact that he/she had either overvoted or undervoted, if the LEO chose to activate this feature. Furthermore, the VOI System eliminated the submission of ballots to the wrong LEO. Finally, voter intent was clearly apparent because the voter used the System to electronically mark the E-Ballot.

Although 100 percent of the data on the submitted EFPCAs was complete and legible, several EFPCAs had to be resubmitted because citizens provided inaccurate information and did not follow digital certificate procedures correctly. For example, Orange County had two applicants who mistakenly listed their current mailing addresses as their legal voting residences. The LEO contacted them and requested that they submit another EFPCA with the correct data. Both applicants electronically resubmitted their EFPCAs on the same day they were contacted, thereby quickly correcting their mistake and ensuring their eligibility to vote in the election. In another instance, a husband and wife used the husband's certificate and password for submitting both of their EFPCAs. This action resulted in her EFPCA being denied because the signature did not match the information submitted on the EFPCA.

Table 4.2-2. How the VOI Design Addressed Ballot Processing Problems

BALLOT PROCESSING PROBLEMS	VOI DESIGN FEATURES
No postmark/invalid postmark	• An automatic electronic "postmark" is attached to each E-Ballot
Damaged ballot	• Electronic transmission eliminates damage caused by postal transit
No signature/nonmatching signature	• The digital signature stands in place of the handwritten signature
No witness address/signature	• The digital signature stands in place of the witness requirement
Mailed to wrong election office	• A voter is only able to request an E-Ballot from the jurisdiction in which he/she is registered. Consequently, when the voted E-Ballot is submitted, the VOI System knows where to return it
Uncounted race attributed to undervoting/overvoting	• An undervoting and overvoting warning message was provided by the system if the LEO activated this feature

4.2.2 The VOI System Significantly Reduced UOCAVA Absentee Ballot Transit Time and Increased Ballot Availability to the Voters

Ballot transit time is the interval between the date that the LEO deposits the UOCAVA ballots in the U.S. mail and the date the returned ballots are received by the LEO. During this interval, the ballot may be transported by military and overseas postal systems in addition to the U.S. Postal Service. Transit time also includes the time the ballot is in the possession of the voter, that is, from delivery to his/her mailbox until he/she places it back in the mail to return to the LEO. Consequently, there are two elements to consider relative to transit time: the period that the ballot is in the mail system and the period that the ballot is in the possession of the voter.

The UOCAVA Absentee By-Mail Process

The 1996 FVAP Post Election Survey of LEOs and UOCAVA voters cited transit time as a significant obstacle to the participation of UOCAVA voters in the 1996 General Election. As Figure 4.2-3 illustrates, 26 percent of the Uniformed Services who responded to the survey stated that their main reason for not voting in the 1996 General Election was that their ballots either arrived too late to be voted and returned by the deadline or did not arrive at all[14].

The five VOI LEOs reported that for the November 2000 Presidential Election between 1 and 7 percent of the total returned UOCAVA absentee by-mail ballots were received after election day. The percentage of ballots not returned at all was much higher, ranging from 22 to 83 percent.

---

14 One reason for not receiving a ballot at all could be that the citizen did not request an absentee ballot.

Figure 4.2-3. Percent of UOCAVA Survey Respondents Who Cited Not Receiving the Absentee By-Mail Ballot in Time to Vote in 1996 as the Main Reason for Not Voting
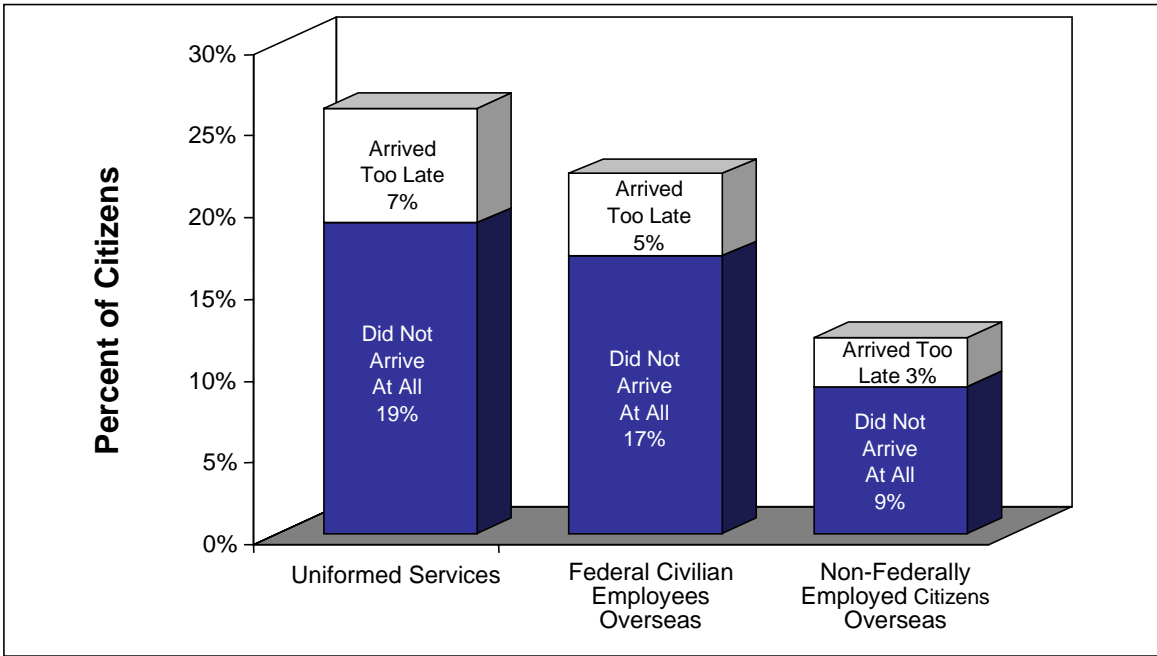
Source: FVAP 1996 Post Election Survey Final Report

Sixty-nine of the VOI voters also returned a by-mail ballot; seven of these were received after election day. Figure 4.2-4 shows the average ballot transit time for the VOI voters who also submitted paper ballots by mail. The average transit time was based on a small number of voters in each participating county and therefore does not reflect the average transit time for all UOCAVA voters. The fact that there were a small number of overseas voters in the Pilot could be the reason why the average overseas transit time in Orange County, Florida, and South Carolina was less than the average domestic transit time.

The VOI System

One of the obvious anticipated benefits of the VOI System was the reduction of ballot transit time because transmission of information over the Internet is essentially instantaneous. Figure 4.2-5 shows the average ballot transit time for the VOI electronic ballots. This period includes the time it took for the voter to request, download, vote, and return the ballot.

In addition to ensuring that the ballots can be received by the voter and returned by the deadline to the LEO, the reduced time in transit has the result of making the ballot available to the citizen for a longer period. For the 2000 General Election, absentee ballots were ready in the VOI jurisdictions about 45 days before election day. Had the E-Ballots been loaded on the System at that time, the VOI voters could have downloaded a blank ballot to use as a sample ballot and become familiar with the candidates and questions. This would have provided a more comparable experience to that of in-person voters who receive sample ballots and other election-related materials in the months leading up to the election.

Figure 4.2-4. Transit Time for By-Mail Ballots for U.S. and Overseas VOI Voters in the 2000 General Election[15]
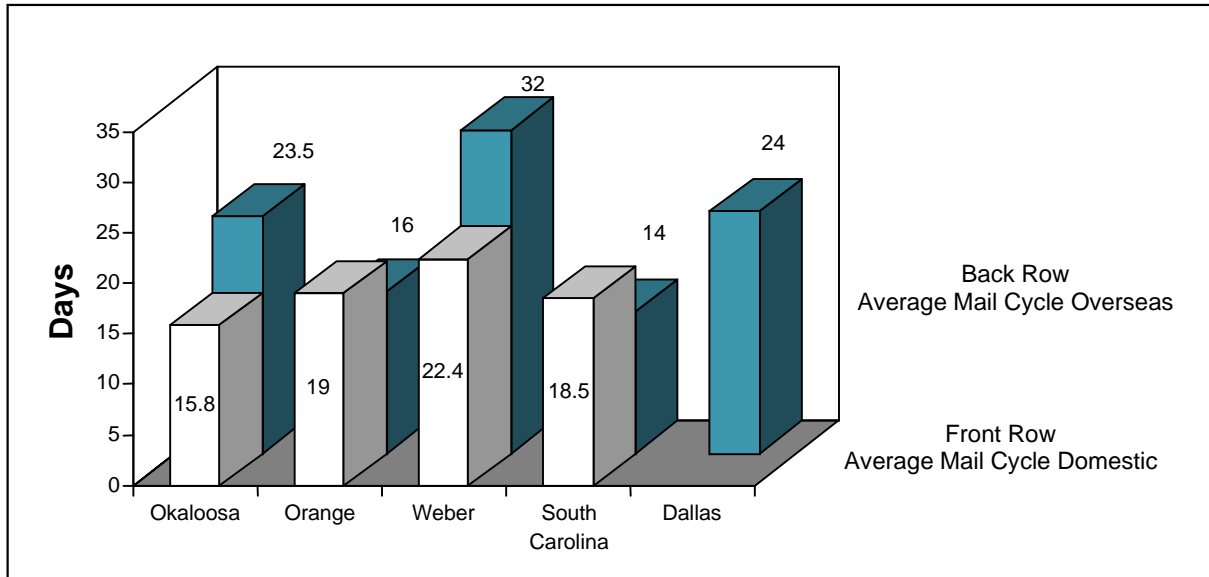
Figure 4.2-5. Transit Time for VOI Electronic Ballots for U.S. and Overseas VOI Voters[15]
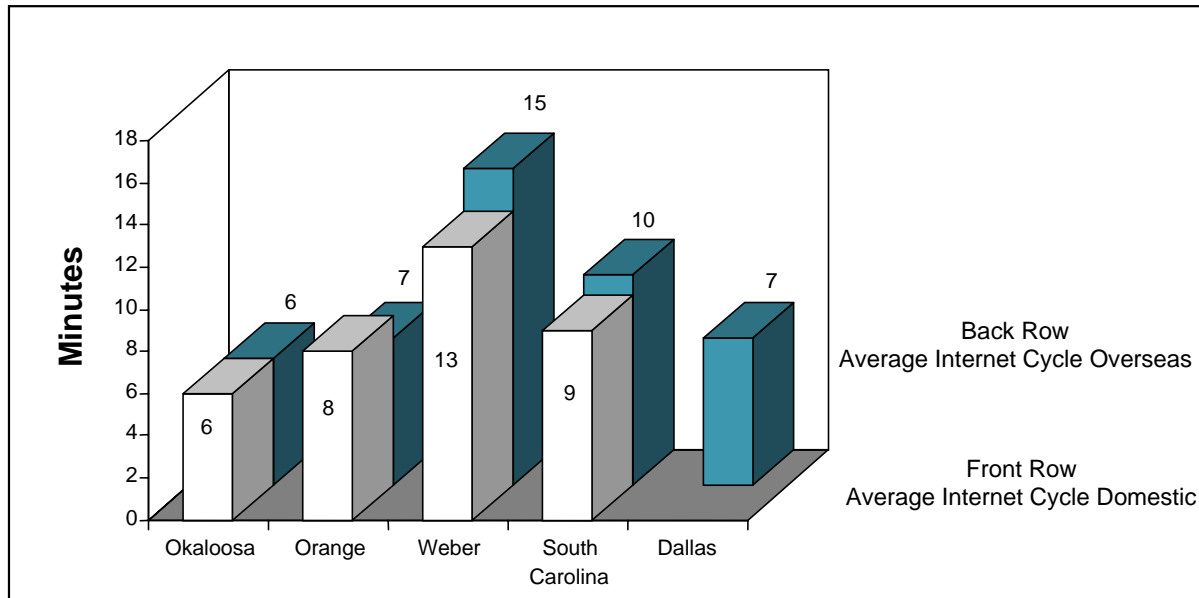
One Pilot participant commented that "…not having to mail the ballot many days ahead of the election is much better and gives more time to research candidates and issues to vote on." This

---

15 Dallas had only one voter, who was located in Turkey; therefore, the number provided is an actual for the single voter.

process is especially helpful to overseas voters because election information, particularly on the state and local level, is not as readily available overseas as it is in the United States. Twenty-five VOI participants downloaded a blank ballot that they did not vote and return, then later downloaded a second blank ballot that they did vote and return. These participants might have wanted time to review the ballot before voting.

In addition to providing a longer time period for the UOCAVA voter to become informed, the longer ballot availability period may also translate into greater enfranchisement for these voters, particularly military personnel. The mobility of military voters has been one of the principal challenges to the absentee by-mail voting process. It is standard practice for military personnel to change their duty stations approximately every 2 years. Neglecting to notify their LEOs of these address changes is a frequently cited cause for ballots being returned as undeliverable. However, the significant reduction of Armed Forces personnel and the closing of many overseas bases over the past 10 years have added a new dimension to the mobility issue.

As discussed in Section 4.2.4, this drawdown in force structure has resulted in a significantly increased rate of deployment to respond to national defense requirements. Therefore, military service personnel are away from their home bases more frequently. Even in the situation where the LEO has a current home base address, the service member may not be there when the ballot arrives and may not return in time to vote and return the ballot. One VOI participant was an Air Force pilot stationed in the U.S. who registered and was approved to vote absentee from his U.S. base location. However, he was subsequently sent on a short-term deployment to Saudi Arabia and took his VOI materials with him. Because his actual physical location was not relevant in the VOI System, he was able to access the System and vote from his overseas location. It is unlikely that the by-mail process can be responsive enough to deal with the frequent, short deployment scenario.

Figure 4.2-6 illustrates the time of receipt of the paper and the E-Ballots from VOI participants. It begins on September 26, which was the day that absentee ballots were first available for the November 7 election. Although the translation of paper format ballots to electronic format ballots was relatively easy with the VOI E-Ballot Tool, it was nevertheless an additional activity that the LEOs had to perform at the least convenient time in their work schedules. To avoid expending effort to translate ballot styles that would not be needed, the LEOs did not create and load E-Ballots on their servers until they were relatively certain which particular ballot styles would be required. Consequently, E-Ballots were not available on the System until the second week of October. As a result of this artificiality of the Pilot Project, no meaningful conclusions can be drawn from these data.

Figure 4.2-6. E-Ballots Versus Mailed Ballots Arrival Timeline for VOI Participants (September 2000 Through November 2000)
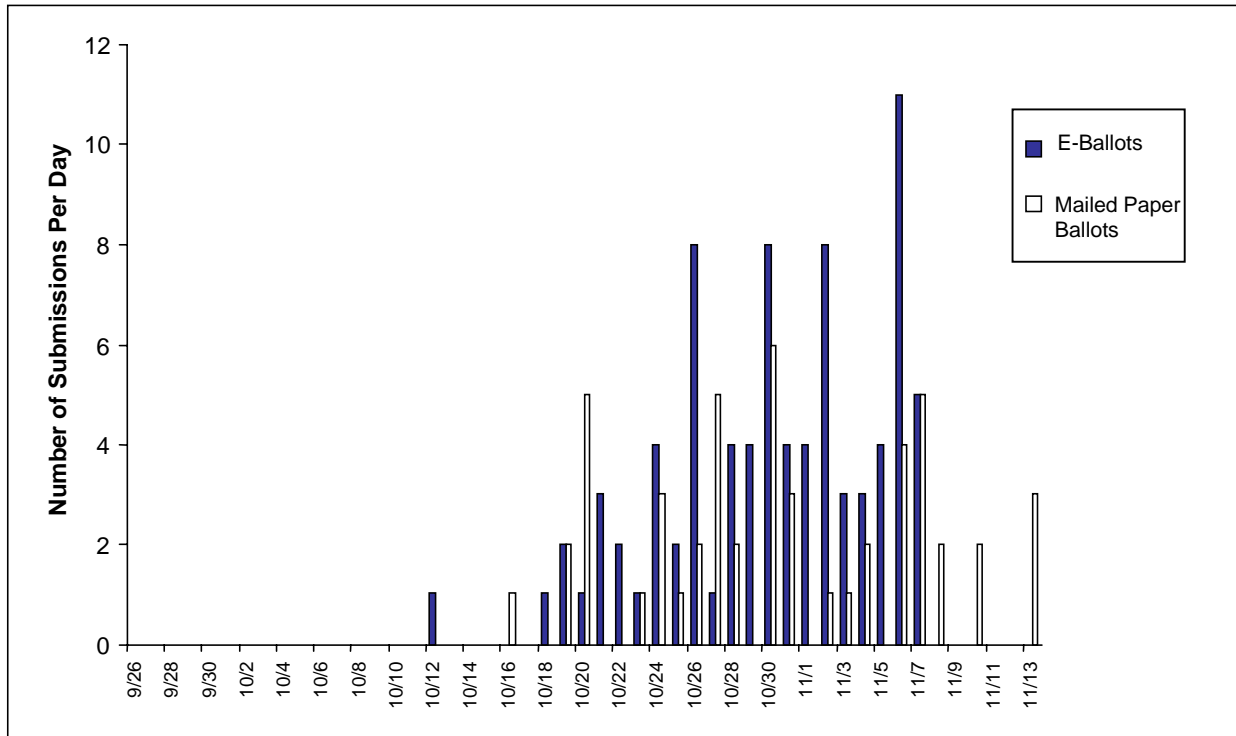
Source: FVAP Server Logs and 2000 Participating LEO Data

4.2.3 VOI System Availability Allowed Pilot Participants to Complete Voting Activities Within the Mandated Time Frame

The UOCAVA Absentee By-Mail Process

With regard to the UOCAVA absentee by-mail election process, availability refers to the ability of the UOCAVA citizen to obtain and execute the necessary registration and voting materials within the mandated time periods. In the by-mail process, the citizen must be able to obtain an FPCA from a Voting Assistance Officer (VAO) or another source, such as the FVAP, and complete and send it to the LEO for receipt approximately 30 days before an election. The LEO is responsible for making the absentee ballots available as quickly as possible so the citizen may receive, vote, and return the ballot by the established deadline.

LEOs must also be available to respond to inquiries from the UOCAVA citizen regarding his/her registration status and the availability of the ballot. For UOCAVA citizens located in the United States, contacting the LEO during business hours may be feasible; however, overseas citizens may not be successful because of differences in time zones. Costs also can be incurred by the citizen from making long distance telephone calls to the LEOs. The FVAP has established toll free numbers to assist citizens, but this adds an additional step and time for the FVAP to contact the LEO and then respond to the citizen.

The VOI Pilot

In the VOI Pilot, the responsibility for delivering election materials to UOCAVA citizens was transferred from the VAOs, FVAP, LEOs, and postal services to the VOI System as the single source for EFPCAs and E-Ballots. Consequently, the availability of the VOI System was extremely important. In the VOI context, availability was defined by the percentage of time that both the FVAP and the LEO servers were online and operating.

The VOI System became operational for EFPCA distribution in January 2000 and for E-Ballot distribution in October 2000. Therefore, VOI System availability was assessed for the entire voting and registration time frame extending from February 2000 until the close of polls in November 2000, with a focus on the E-Ballot availability period from October 2000 until the close of polls. System availability at the various LEO locations ranged from 92.58 to 99.60 percent for the entire registration and voting period (see Figure 4.2-7). From October 2000 until election day, when E-Ballots were available, System availability ranged from 94.90 to 98.80 percent (see Figure 4.2-8). A majority of the outages in LEO server availability were attributed to local communications problems and Internet service provider (ISP) connections. Outages in FVAP server availability were attributed to a planned outage to load and test the software for the transition between Phase 1 and Phase 2 System functionality and general System errors that locked the server on several occasions.

Figure 4.2-7. LEO and FVAP Server Availability Throughout the Registration and Voting Cycle (February 2000 Through November 2000)
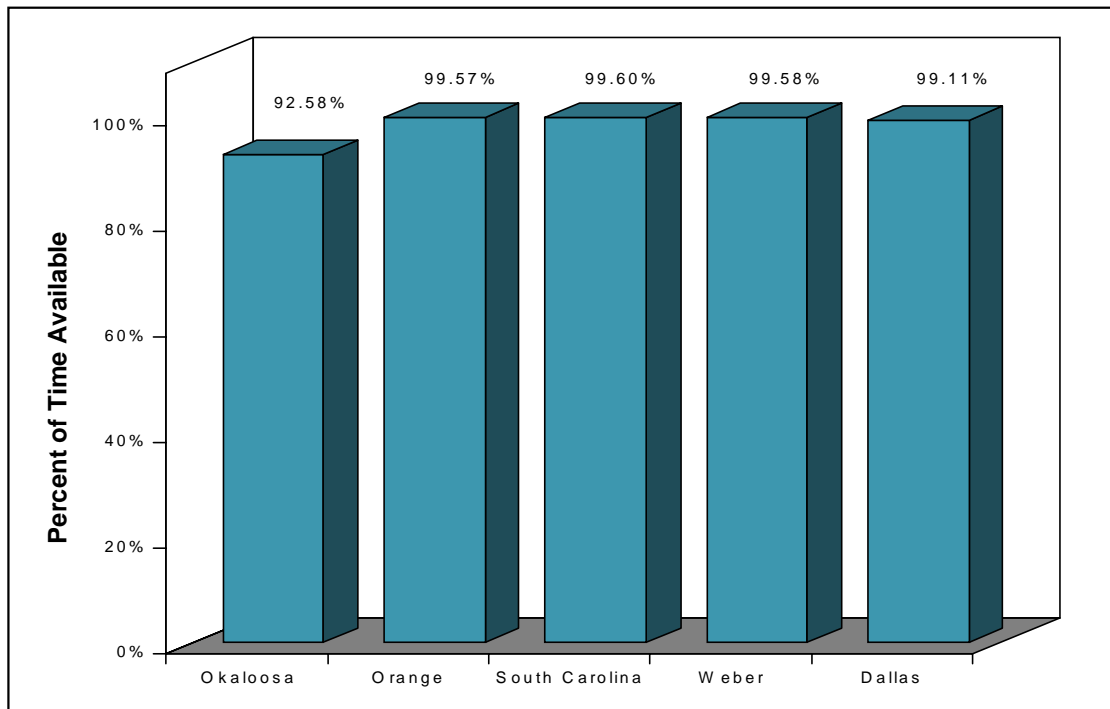
Source: FVAP Server Logs

Figure 4.2-8. LEO and FVAP Server Availability Throughout the Voting Period (October 2000 Through November 2000)
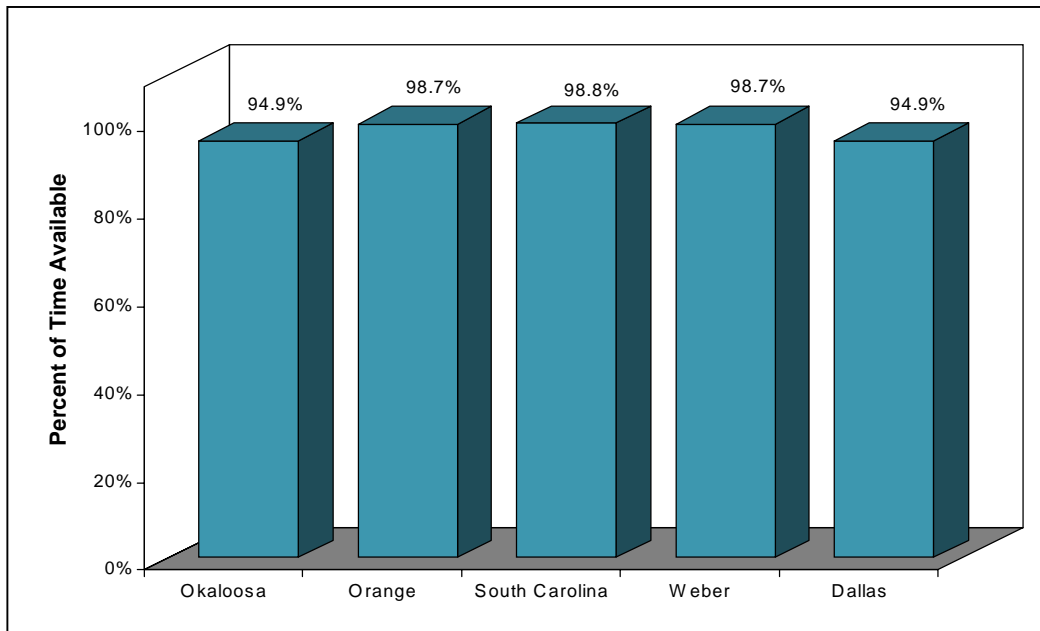
Source: FVAP Server Logs

To maximize the availability of the VOI System, automated features and manual processes were implemented. The System was designed with a pager feature that would automatically notify the FVAP segment administrators if an outage had occurred at either a LEO or the FVAP server site. Furthermore, the FVAP server contacted the LEO servers at regular intervals to verify that they were operational.

In addition, continuous personal attendance of the System by the FVAP system administrators was implemented two weeks before the election as an added reliability feature. This constant physical presence, in conjunction with the use of the pager feature, minimized the amount of time the System was unavailable as a result of unexpected occurrences, including localized ISP and/or power outages. Over the Pilot period, the VOI System experienced several minor localized system outages affecting specific LEO sites. On several occasions, LEO servers went down, or their communications were disrupted, resulting in 14 missed transactions during the course of the Pilot. In three other instances, the FVAP server went down for short periods, possibly resulting in missed transactions.

Although these outages hindered the UOCAVA citizen from executing his/her activity at that time, in all instances the UOCAVA citizen was able to complete the transaction at a later date. Citizens were notified automatically by the System if the transaction failed because of the unavailability of a LEO.

An additional availability problem occurred on election night at one of the Pilot jurisdiction sites. In this instance, two UOCAVA citizens attempted to submit their E-Ballots to the same LEO server within seconds of each other. One of the E-Ballots was voted successfully; however, the other was not because the server had locked up. The system administrator rebooted the LEO

server, contacted the citizen, and requested that he/she resubmit the E-Ballot. The E-Ballot was successfully cast.

Despite these minor problems, analysis of the FVAP and LEO server data and data gathered from interviews with UOCAVA citizens after the election suggest that no citizen was prevented from registering or voting because of unavailability of the VOI System. Furthermore, independent testers assessed the availability of the VOI System and found that the System fulfilled 100 percent of the requirements needed to maintain system availability.

4.2.4 The VOI System Reduced the Registration and Voting Burdens Caused by the High Mobility of the UOCAVA VOI Pilot Participants

UOCAVA citizens do not always remain in the same geographic location during an election cycle. They may not receive mail on a timely basis if they are temporarily away from their base location on deployment. They may not receive it at all if they have moved and election correspondence or the absentee ballot was sent to their previous address. As a rule, absentee ballots are not forwarded by the postal services. Change in user physical location is transparent to the Internet; therefore, the VOI System was able to mitigate some of the mobility issues experienced by UOCAVA citizens.

Many UOCAVA citizens are in their current locations for less than 2 years (see Figure 4.2-9). In addition, trends indicate an increase in deployment for military personnel. As Figure 4.2-10 shows, the pace of U.S. military deployments has changed over the last 10 years as a result of the smaller force structure. The deployment tempo of forces has continued to increase and members of the Uniformed Services are engaged in shorter, but more frequent, deployments. Information indicates this trend continues today. As the military experiences shorter deployments with less notice, military voters are experiencing greater difficulty registering and voting for several reasons, including being away from the locations where their mail is normally delivered and frequently changing their mailing addresses. These difficulties may prevent them from voting.

Figure 4.2-9. Percent of UOCAVA Citizens in 1996 Who Have Resided in Current Location Less Than 2 Years
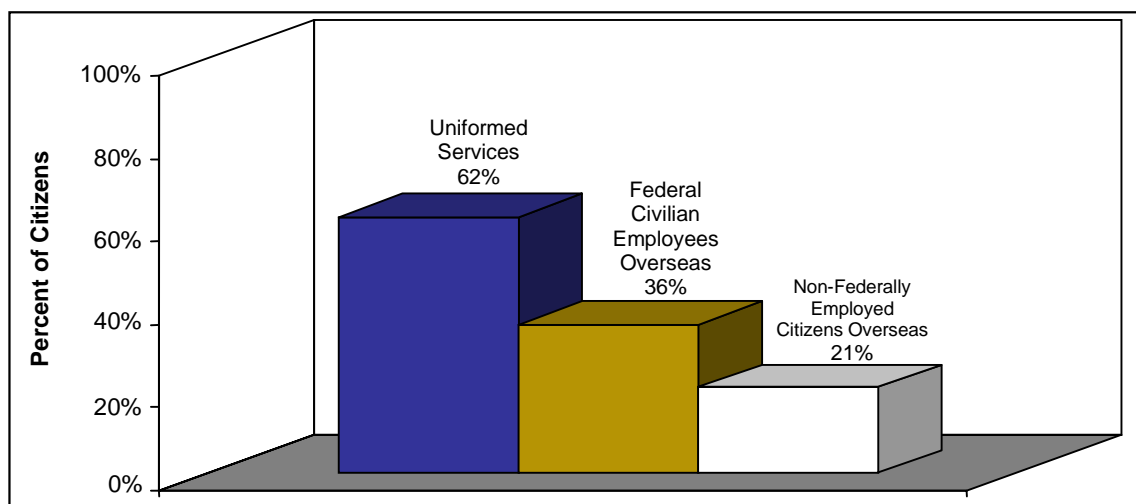
Source: FVAP 1996 Post Election Survey Final Report

Figure 4.2-10. Smaller Force Structure Increases Deployment Tempo
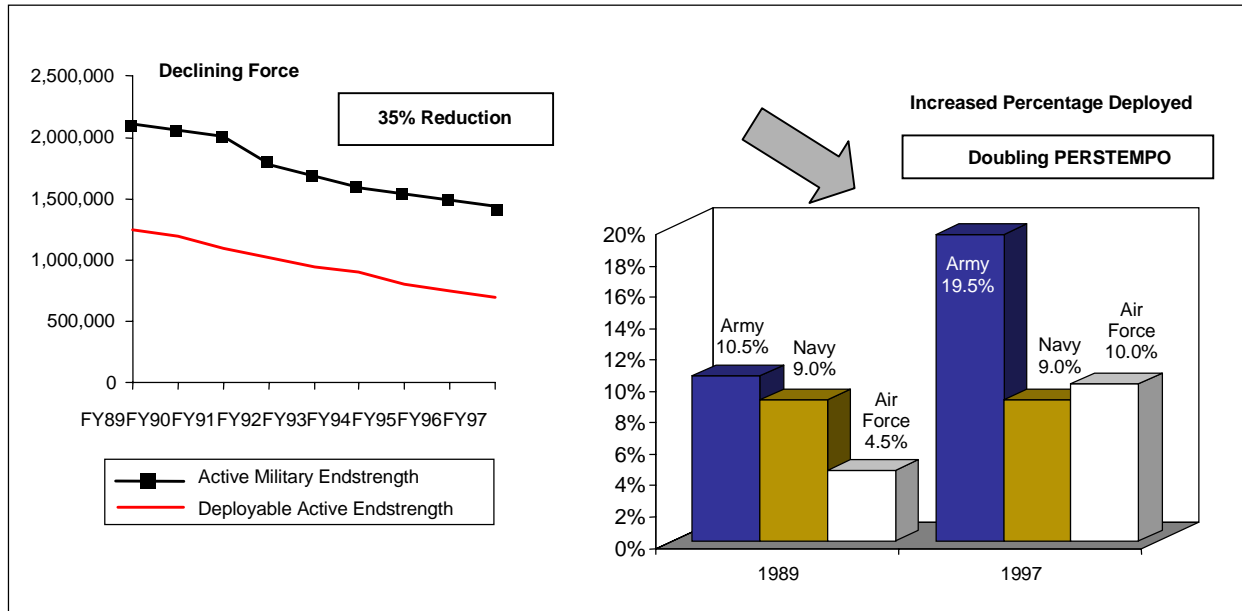
Source: FY2001 Defense Budget Briefing, William J. Lynn, http://www.ndia.org/events/proceedings/073/Lynn.pdf

The UOCAVA Absentee By-Mail Process

Citizens who are permanently relocated, deployed, or on emergency leave at critical times during the election cycle find the by-mail process challenging. Mailing addresses are quickly outdated, and voters are sometimes unable to receive their voting materials in the mail in time to register or vote. LEOs participating in the VOI Pilot noted that citizens often do not send their updated address information before the election, which prevents them from receiving the ballot.

The VOI System

The VOI System enabled citizens to register or vote regardless of physical location. All necessary forms were available on the VOI System and could be obtained at the citizen's convenience.

Seven participants who responded to VOI interviews changed their physical addresses during the election period but were still able to participate in the VOI Pilot without any difficulty. In two instances, citizens registered from one location and voted from another. This might not have been possible in the by-mail process, depending on whether the citizen provided the LEO with a change of address form in a timely manner.

The experience of one VOI voter deployed in the Middle East demonstrated how the VOI System could improve the UOCAVA absentee voting experience for citizens who are frequently away from their base locations. This participant was away from his base location for weeks at a time on various military assignments. Consequently, it was extremely difficult for him to receive the necessary forms and vote using the UOCAVA absentee by-mail process within the election time frame. However, he was able to vote using the VOI System without any difficulty.

Another participant had to take emergency leave during the election cycle. As a result of this sudden move, the citizen was unable to receive UOCAVA absentee by-mail materials at his temporary location because they were sent to his duty station address. However, using the VOI System, the citizen was able to vote from his temporary location.

In order to use the VOI System to address these mobility issues, VOI Pilot participants needed to access the Internet from their various geographic locations. UOCAVA citizens participating in the Pilot represented a broad geographic footprint, yet all participants had access to the Internet. Twenty-six percent of the VOI Pilot participants were overseas. The 91 voters who registered did so from 21 states and U.S. Territories, 11 countries in Europe, the Middle East, and the Far East. Of the 32 eligible voters outside the United States, 21 registered and 21 returned voted E-Ballots. Of the 95 eligible voters in the United States, 70 registered and 63 returned voted E-Ballots. As illustrated by Figure 4.2-11, participants from 21 states and territories and 11 countries used the VOI remote registration and/or voting capability, demonstrating that the Internet could be used to meet the needs of a geographically dispersed UOCAVA population.

Figure 4.2-11. VOI Pilot Participants Who Registered and/or Voted by Location
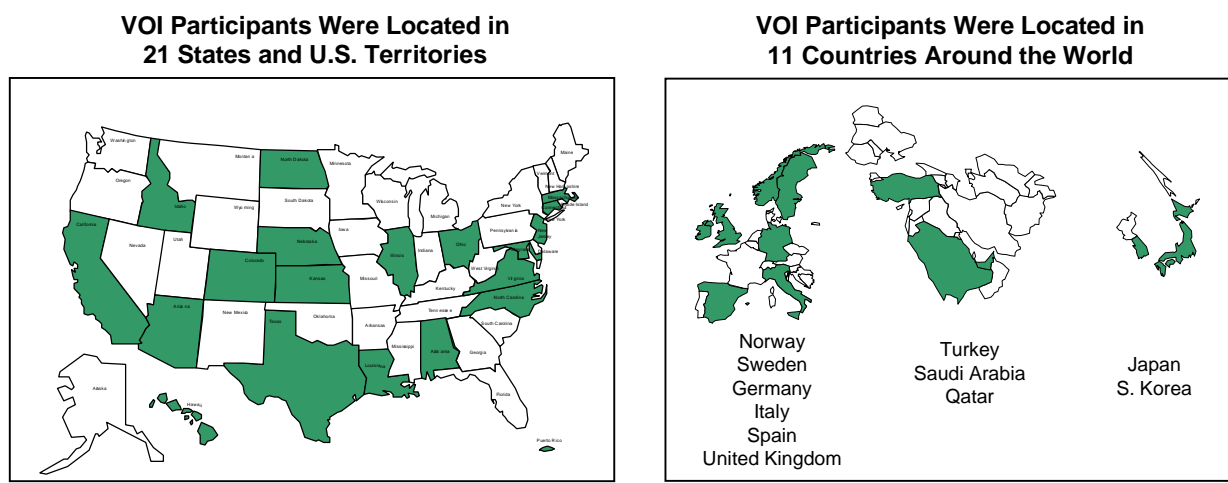
Source: VOI Participant Data   *Source: VOI Participant Data*

4.2.5   As a Centralized Source of Information, the VOI System Provided an Opportunity for an Improved Understanding of UOCAVA Absentee Registration and Voting Processes

The UOCAVA Absentee By-Mail Process

Currently, UOCAVA citizens' participation in the absentee voting process is reduced as a result of a lack of information and limited familiarity with the procedures related to UOCAVA absentee by-mail voting. The primary reason for not voting, as cited by UOCAVA citizens in the 1996 FVAP Post Election Survey, was not knowing how to get an absentee ballot. Another reason cited for not voting was not knowing whether they were eligible to participate (see Figure 4.2-12). The citizens also reported a lack of consistency in election-related information attributed to multiple information sources.

**Figure 4.2-12. Nonvoting UOCAVA Citizens' Reasons for
Not Participating in the 1996 Election**
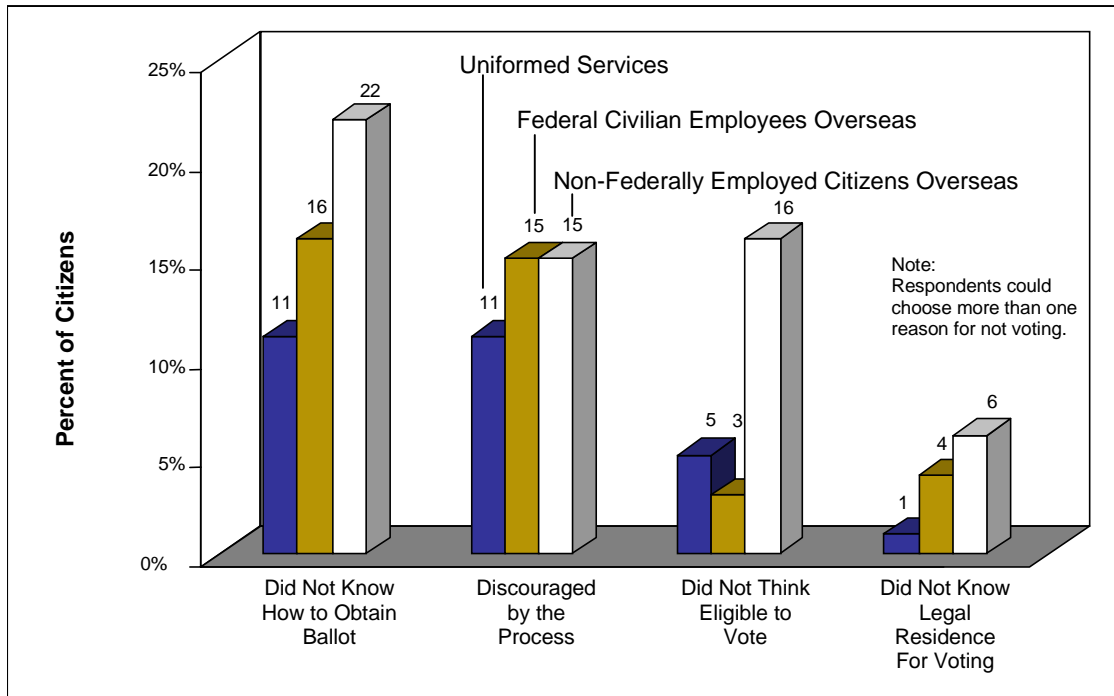
Source: FVAP 1996 Post Election Survey Final Report

Although newly registered UOCAVA citizens are supposed to receive notification by mail to confirm their registration status, not all citizens receive this confirmation. Based on the 1996 FVAP Post Election Survey, an average of one-third of the UOCAVA citizen respondents did not receive notification that their ballot requests arrived at the LEO (see Figure 4.2-13). Although this does not necessarily mean that they did not receive their ballots, it can cause the voter undue concern and additional effort to clarify his/her registration status.

Figure 4.2-13. UOCAVA Citizen Receipt of Notification that Ballot Request Was Received in the 1996 Election
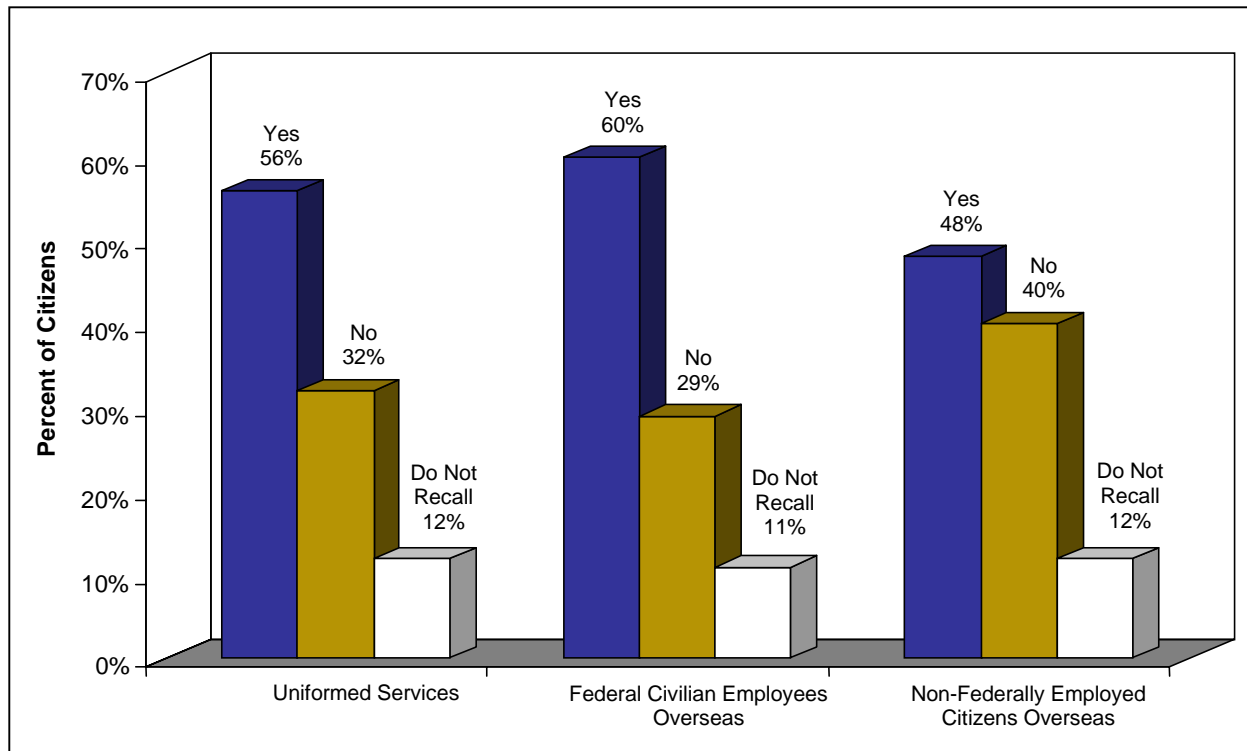
Source: FVAP 1996 Post Election Survey Final Report

The VOI System

As the single source for forms and instructions, the VOI System simplified the process for citizens to locate election information and materials. Table 4.2-3 compares the means by which information was provided to citizens in the by-mail process and the VOI process.

Table 4.2-3. Methods for Receiving Information for UOCAVA Voters

INFORMATION REQUIRED	BY-MAIL PROCESS	VOI SYSTEM
Absentee registration materials	• VAO, embassy, consulate, FVAP, advocacy organizations abroad, LEOs	• VOI System
Ballot	• LEOs	• VOI System
Absentee registration and ballot submission dates	• LEOs, election materials, FVAP, VAO, VAG, embassies, consulates	• VOI System
Methods of communication with election officials	• E-mail, phone, fax, mail, FVAP	• VOI Help Desk, e-mail, phone, fax
Absentee registration and ballot completion instructions	• FPCA, ballot packet, LEO, FVAP, VAG, VAO	• Citizen information packet, VOI software, VOI Help Desk
Absentee registration/ballot receipt confirmation	• LEOs, FVAP	• VOI Check Status feature

In the VOI System, all participants were provided with a Help Desk number to call with any technical issues, and with LEO and FVAP e-mail addresses and phone numbers for any other assistance they required.

Enabling Pilot participants to directly confirm their registration and voting status proved to be a useful System feature. System activity logs showed that 96 percent of participants used the Check Status feature at least once. Of the citizens interviewed at the conclusion of the Pilot, 28 felt more informed by using the VOI System than the UOCAVA absentee by-mail process (see Figure 4.2-14).

FVAP server log data indicated that Pilot participants used the Check Status feature more frequently as the election deadline drew closer. This feature not only assured citizens of their eligibility to vote status, but also reduced the burden on LEOs to respond to registration status requests during the busy period before the election deadline.

The VOI System was a pilot project. Because it was the first attempt to implement an Internet voting program, the distribution of information to citizens required considerable effort from the FVAP program management team. This level of effort to distribute information could not be replicated in a larger scale system. The FVAP sent the Pilot participants software and system documentation via commercial carrier or registered mail, which was a time-consuming and expensive process.

Figure 4.2-14. Citizen Response to Post Pilot Interview Questions Comparing Information Levels Using the By-Mail Process and the VOI System
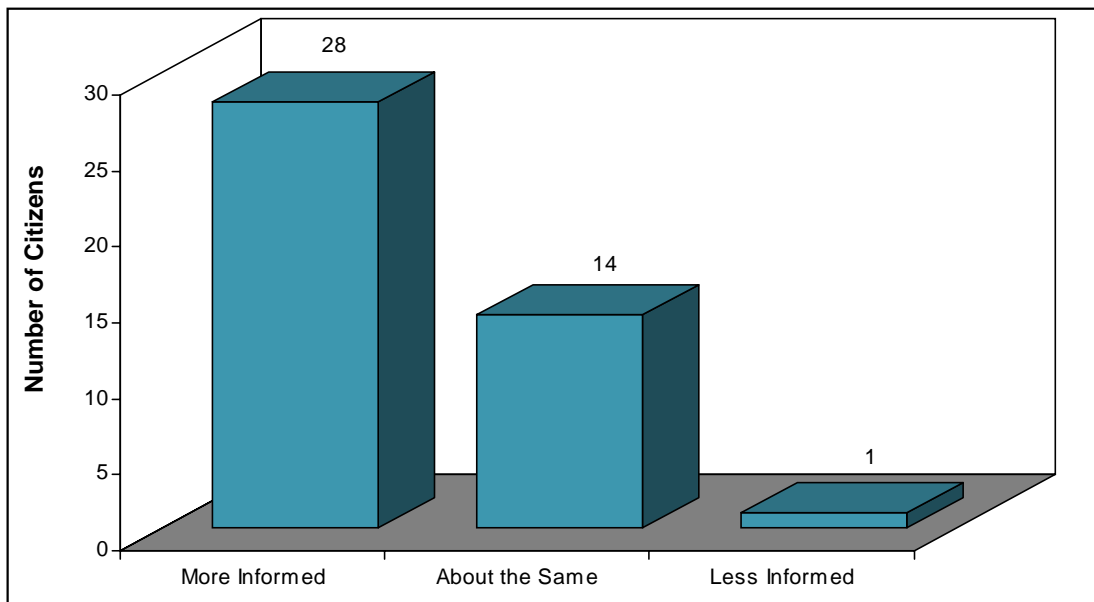
Source: VOI Participant Interviews

4.2.6 Overall, the VOI System Increased LEO Workload

The UOCAVA Absentee By-Mail Process

With the UOCAVA absentee by-mail process, the LEOs must spend considerable time distributing various election materials; mailing paper ballots to registrants; preparing and sending correspondence to citizens who have submitted incomplete or invalid FPCAs or ballot materials; opening voted absentee ballot envelopes; and responding to letters, phone calls, and e-mail from citizens who have inquiries, problems, or simply want to check on the status of their FPCAs or absentee ballots.

The VOI System

Although automation reduced the administrative burden on the LEOs in some instances, it increased the workload in other areas. The VOI System overall increased the LEO workload because it was an additional activity to their normal administrative process. As discussed above, the VOI System was intentionally designed not to integrate with the current UOCAVA absentee by-mail processes. This design caused the LEOs to perform some redundant administrative duties in the automated and manual processes. For example, the E-Ballot Tool was developed to assist the LEOs in their E-Ballot construction for the VOI Pilot. However, this was still a duplicate process of the absentee by-mail ballot generation activity.

The VOI System has the potential to reduce the amount of time election staff spend on these tasks by automating the registration, status checking and ballot delivery process. Through this System, LEO efforts for many activities listed above were significantly reduced. For example, to register and request an E-Ballot using the VOI System, the citizen simply logged on to the System and his/her request was automatically processed. The citizen could retrieve election materials and status information at his/her convenience, freeing the LEO from this citizen-by-citizen task.

The FVAP server also fulfilled the citizen identity validation responsibilities. When the E-Ballot was received at the FVAP server, the digital certificate was verified against the PKI certificate revocation list, providing authentication of the voter's identity. In the UOCAVA absentee by-mail process, the LEO must manually compare the handwritten signature/address and witness signature/address on the election materials with the signature on file. This time-consuming activity was reduced through VOI automation.

The VOI design did not include tabulation capabilities or interfaces with existing tabulation systems. This required the LEOs to print out the E-Ballots and transcribe them onto the standard absentee by-mail ballots for tabulation. Both activities were time consuming and offset some of the workload benefits.

All the LEOs who participated in the VOI Pilot expressed an interest during the VOI interviews in continuing their use of the VOI System despite the redundancies in the administrative duties between the by-mail process and the VOI System. They all acknowledged that design enhancements for a future larger scale system could mitigate many of the issues discussed here.

4.3 THE INTRODUCTION OF TECHNOLOGY IN THE UOCAVA REGISTRATION AND VOTING PROCESS CREATES NEW CONSIDERATIONS

Although the VOI System provided increased flexibility and service to the Pilot participants, the enabling technology providing these benefits did introduce additional complexity to the election administration process. It also introduced new threats that are not present in the UOCAVA absentee by-mail process. These threats, such as hacking, spoofing, and viruses, stem from the use of the Internet.

4.3.1 VOI Pilot Participants in Most Cases Were Comfortable With Configuring and Using a Personal Computer To Access the VOI System

To access the VOI System, Pilot participants needed to install the necessary software, configure their computer systems for use with the VOI System, use an Internet-based application, and use the digital certificate. In VOI interviews, 44 voters responded that they voted from home, work, or both. A majority of the respondents were able to vote from their home computers because their hardware met the configuration requirements of the Pilot. Some respondents answered "both" to the question because they were able to configure their work and home computers to access the VOI System (see Figure 4.3-1).

The number who voted from home indicates a high level of familiarity with computers among the participants. This was confirmed by the participant interviews that were conducted after the VOI Pilot voting period ended. Figure 4.3-2 shows that 44 VOI participants who responded to the question regarding comfort levels stated that they were either very comfortable or extremely comfortable using computers. Through online questionnaires, VOI participants responded that they primarily used their computers for e-mail, word processing, and online research.

Figure 4.3-1. Locations of VOI Citizen Workstations
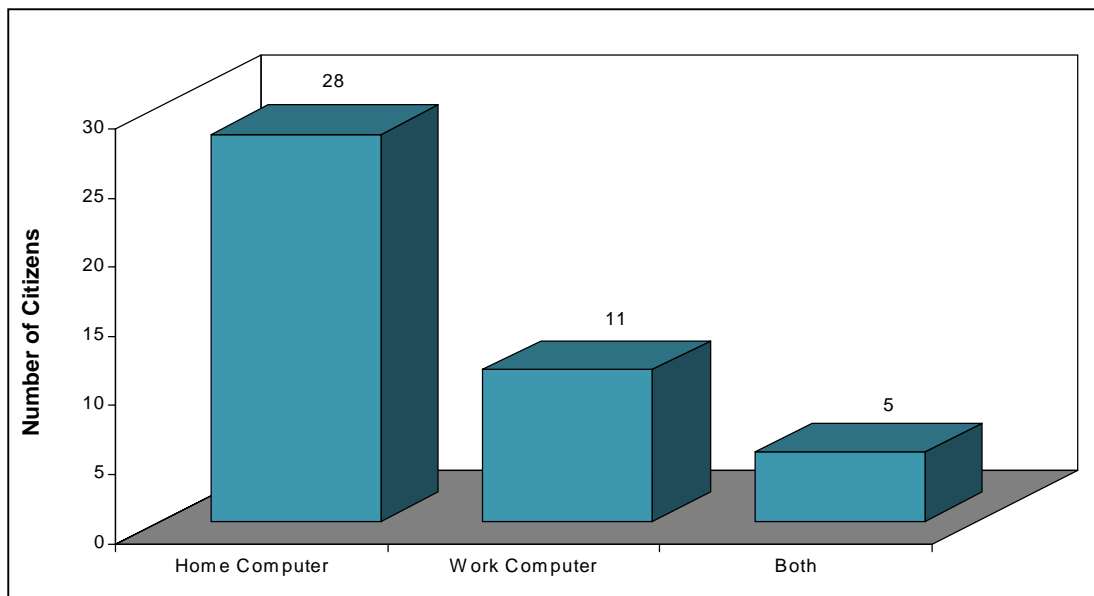
Source: VOI Participant Interviews

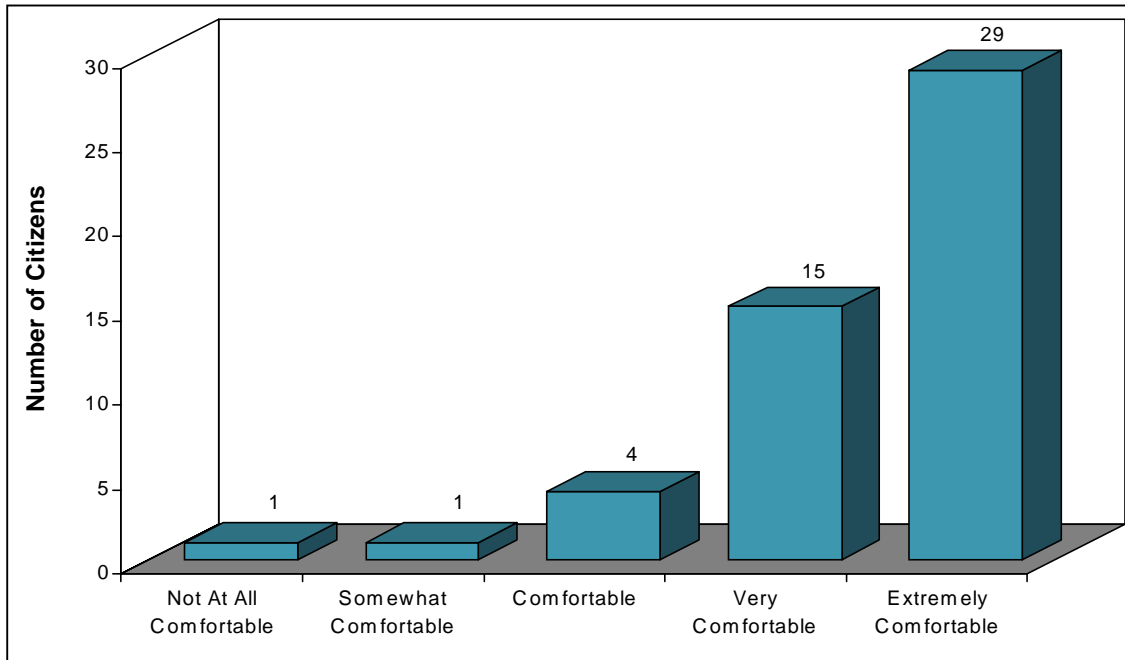**Figure 4.3-2. Citizen Comfort Level Ratings for Working With Computers**

Source: VOI Participant Interviews

All Pilot participants who used their home computers were able to configure their systems for VOI System use without difficulty. Ninety-five percent of Pilot participants who responded to interviews stated that they found installing the software an easy to extremely easy process. Among the remaining 16 respondents to the interview questions who used the System to register and vote, 11 used computers from work and 5 from work and home. Ten citizens had to obtain system administrator approval to install the VOI software (the Netscape Navigator browser and the citizen plug-in).

The Air Force and the Coast Guard have adopted Internet Explorer as their standard browser software. The Air Force allows the installation of Netscape Navigator on an exception basis when it is required for a specific application. The Coast Guard does not have an exception policy and would not permit the installation of Netscape Navigator on its computers. Consequently, several Coast Guard personnel who did not have their own computers had to drop out; the remainder used their home computers.

The Air Force also requires that all custom applications, such as the citizen plug-in, undergo its internal software certification process. The FVAP did not become aware of this requirement until the Summer of 2000, when it was too late to complete Air Force certification before the voting application needed to be available for use. Because the software was scheduled for both DoD and State of Florida certification testing, the Air Force administratively waived this requirement, based on the small scale and one-time use of the Pilot.

Nearly all Federal government computer systems are under fairly strict configuration management control. This means there is a standard suite of software for all users, and only the system administrator is permitted to install software. Any departure from the standard software

suite must undergo an approval process. In the case of custom applications, this effort may entail reviewing the testing documentation and re-testing the application against the organization's standards and criteria.

Configuration management of computer systems is becoming common in the private sector. It not only helps protect against the introduction of viruses and other forms of malicious code but also serves as a good business practice for managing assets. Any future expanded use of a VOI type of application will have to take these requirements into account.

The ability of Pilot participants to use an Internet-based application effectively was demonstrated by the fact that nearly all of the voters submitted ballots successfully. The sole exception was one participant who thought he/she had completed the ballot submission process by voting his/her ballot. He/she did not click the "encrypt and submit" button as required to complete the submission process.

The high level of familiarity with computers and software among VOI Pilot participants is not representative of the general voting population. The participants were self selected, and the Pilot required citizens to have access to a computer; therefore, it is likely that citizens willing to volunteer in an Internet voting pilot had previous experience with computer technology.

4.3.2 VOI Pilot Participants Were Not Familiar With the Use of Digital Certificates

Although the VOI Pilot participants had a high degree of familiarity with computers, they had limited experience with digital certificates. More than one-third of all Help Desk calls related to fulfilling and using the digital certificate. This represented the highest percentage of questions for any component of the VOI System. About one-half of the citizens had to have a new certificate issued. Two-thirds of these had to be reissued as a result of forgotten passwords. The other third had to be reissued because the certificate documents expired before the certificate was downloaded.

Another difficulty was the downloading and exporting of two certificates from a shared computer. This procedure required additional system configuration steps. Three of the 19 married couples that participated in the Pilot contacted the Help Desk regarding this difficulty. One of these couples became discouraged and chose not to continue with the Pilot due to this problem. In another instance, one spouse did not vote using the System because it was too difficult to reconfigure the workstation and download a second certificate.

The problem occurred when two citizens tried to download their digital certificates to the same computer using Netscape Navigator. Because both voters were using the same browser profile, both certificates would be stored in the same location. This caused the process of exporting the certificates to a floppy disk to be confusing. Depending on the steps taken, it could also prevent the downloading of the second certificate. Because the Help Desk was available to explain how to work through the download and export process, both voters could download their certificates and proceed with using the System.

4.3.3 Although the Internet Provides Improvements to the UOCAVA Absentee Registration and Voting Process, It Also Introduces New Security Concerns

Using the Internet to conduct an election inherently introduces new risks to the election system. Denial of service attacks, Trojan horse attacks, and automated vote buying and coercion are all potential risks that the Internet introduces to the voting process.

During a denial of service attack, a malicious hacker overflows a server with requests, causing the server to shut down and deny the availability of the server to its legitimate users. If a large-scale denial of service attack were to be launched at the VOI System during an election period, the citizen's ability to vote could be affected. This is a possibility because several large commercial Web sites have undergone similar attacks, causing their servers to shut down for several days at a time.

The fact that the VOI System used a 30-day voting period—rather than a single day—reduces this risk somewhat because it is unlikely that the perpetrator could sustain an attack for this long. Voters could still use the server at a later time when it has been restored to operation. However, there is still the possibility that a denial of service could take place close to or on election day, a time when a large number of citizens might want to vote.

Although the VOI System could have been vulnerable to such an attack, the System was not widely publicized and no attempts were detected. It can be assumed that if this System had been widely publicized, it would have been a more attractive target because of the prospect for hackers to influence the outcome of the election or to cause embarrassment to the government and political organizations.

Another risk associated with the Internet is a Trojan Horse attack. A Trojan Horse attack could occur after a citizen inserts his/her digital certificate into his/her workstation and types his/her password. Trojan Horse malicious software installed on the computer could intercept the user's keystrokes. The malicious software could then modify the citizen's selections and relay the data back to the malicious hacker. Although the security of the voters' workstations was considered outside the scope of this project, no use of Trojan Horses was detected during operation of the System.

While the possibility of vote buying and undue voter influence is not a new concern, Internet voting provides the opportunity for election fraud on a much larger scale than possible with paper ballots. A system administrator or other third party could monitor a voter's keystrokes using commercially available software to determine how he/she voted. This could provide a vote buyer with verification that the voter made the required ballot choices before payment is made. Employers with an interest in knowing how employees vote could use this technology without the employee's knowledge. These types of software tools combined with the connectivity of the Internet make it possible for a single person to have significant impact.

The VOI Peer Review Group put considerable emphasis on these risks and the lack of available methods to prevent their occurrence. They acknowledged that the nature of both the absentee by-mail and VOI processes necessitates a risk management approach. Tradeoffs may need to be

considered between a high degree of security and providing easier access to the electoral process for UOCAVA citizens.

For the purposes of analysis and discussion, the peer reviewers divided the voting process into three parts: voter registration, delivery of the blank ballot to the voter, and the return of the voted ballot to the LEO. The group agreed the VOI System effectively improved absentee registration and ballot delivery with an acceptable level of security. They observed that the voter identity assurance provided by the use of DoD PKI digital certificates provided a marked improvement to the by-mail registration process.[16] Electronic transmission of the blank ballot was viewed as a low risk method of ballot delivery that reduced LEO-to-citizen transit time to minutes and afforded the citizen more time to review the ballot before casting his/her vote.

The return of the voted ballot is where most security attacks and fraud attempts are likely to occur. Since there are no methods currently available to prevent or effectively counteract many of the cyber threats identified above, the peer reviewers expressed the consensus view that the integrity of the voted ballots could not be adequately assured by a remote Internet voting system on a large scale.

---

16   One of the reviewers characterized the VOI online registration method as a "best practice" in his testimony at the Senate Government Affairs Committee hearing on voter registration reform.

5.0 LESSONS LEARNED AND SCALABILITY ISSUES

The Voting Over the Internet (VOI) Pilot provided valuable insight into the issues that must be considered for broader use of remote registration and voting for UOCAVA citizens via the Internet. The following discussion highlights these issues and presents the challenges and opportunities that lie ahead. The lessons and scalability issues have been organized into three general categories: People, Process, and Technology Issues.

5.1 PEOPLE RELATED LESSONS AND SCALABILITY ISSUES

5.1.1 Volunteer Citizen Recruitment Was Complex

A significant level of effort was required to identify citizens to participate in the VOI Project. The Pilot was designed to support a specific community and because of its scope, the candidate pool was further limited to UOCAVA citizens who resided in one of the five participating jurisdictions. Stated another way, the FVAP was required to find UOCAVA citizens from throughout the world who were eligible to vote in a small number of the more than 3,000 counties in the United States. The recruitment process was further complicated by the inability of the LEOs to link the place of voting residence to current physical locations because of the mobility of this population.

The FVAP focused its recruiting efforts on the Uniformed Services and relied on the Service Voting Action Officer within each of the individual services to help identify possible participants. However, they could not link the current physical location with the place of voting residence of citizens. Consequently, the FVAP and LEOs had to identify potential participants through a time intensive search and sort process.

The manner in which UOCAVA citizens would be recruited for future projects may be very different, depending on the scope. The FVAP would work cooperatively with state and local election officials in all the participating jurisdictions to develop a promotional program to maximize outreach to eligible UOCAVA citizens. The Pilot utilized many avenues to publicize the project: military publications and Web sites, announcements at FVAP training sessions, articles in national and international newspapers and contact with overseas citizen advocacy organizations. The marketing model would be revised to account for a larger scale effort, and these resources could be employed in a different manner.

5.1.2 Computer Access Is a Mixed Issue for Specialized Software Applications, Such as Internet Based Registration and Voting

Uniformed Service members have a high rate of access to personal computers and the Internet at their workplace. However, in most workplace situations, the VOI voters did not have the authority to change the browser version or to add the VOI software. DoD computers are under strict configuration management that does not permit users to add or modify computer applications. In some cases, system administrators authorized installation of the VOI software. In other instances, several volunteers had to drop out of the Pilot. This was particularly the case with the Coast Guard volunteers. The Coast Guard uses Microsoft's Internet Explorer browser,

which was not compatible with the VOI System. Loading the Netscape Navigator browser was not permitted under its configuration management policy.

Future Internet registration and voting system initiatives would explicitly account for this need to coordinate with government network administrators, thus allowing timely certification and inclusion of VOI software. Additionally, strongly enforced network configuration management protocols could translate into a substantial positive factor. One of the biggest challenges for remote voting systems is the threat of malicious software resident on the citizen's personal computer. Rigorous configuration management protocols greatly mitigate that threat. There appears to be a trend for other Federal agency and private sector computer systems to be placed under similar strict configuration management control.

5.1.3 Computer Installation Issues Affected the Participant's Perception of Ease of Use

The installation of the registration and voting application should be intuitive and as familiar as the installation of ordinary browser-based applications (e.g., Adobe® Acrobat® Reader® plug-in). For the Pilot, the citizen was required to install a furnished browser and a custom plug-in application from a CD-ROM. This increases the level of effort required by the citizen and in some instances will be beyond the user's technical capability which could lead some to decide that the benefit of remote registration and voting is not worth the effort.

For future initiatives, installation procedures will be comparable to those associated with commercial best practices. Topics to be addressed include the easy and secure downloading of the browser plug-in application, an easy-to-use and robust installation program for the plug-in application, and configuration guidance for browser Java™ and JavaScript™ capabilities.

5.1.4 Different Staffing Profile for Operating a Remote Registration and Voting System May Be Required

The introduction of technology for UOCAVA citizen registration and voting may have a significant impact on the staffing model for supporting such a system. Currently, election day activities are supported by staff that transfer voting equipment from warehouses to poll locations; set up and test the equipment; and following its use, return the equipment to storage. These activities can use personnel without any specialized technical skills. Although some of this voting equipment employs computer technology, it was explicitly designed to allow operation by non-technical professionals.

As advanced technology is introduced to provide new registration and voting capabilities, the new systems have the potential to require a significant change in the skill sets required on a year-long basis (e.g., full-time NT operating system administrator). For the Pilot, limited attention was given to this logistical life-cycle consideration. It was decided that the development team would serve as the VOI "system administrator," and this decision greatly mitigated any impact on LEO staffing requirements.

For future initiatives, considerable attention would be directed toward minimizing the number and nature of activities that would be required of a highly specialized staff. One approach is to develop what is commonly referred to as an embedded computer system. In other words, the

registration and voting system could be engineered so that some of the traditional computer system administrative functions performed by specialized staff either would be eliminated or could be performed by typical local election staff.

5.2 PROCESS RELATED LESSONS AND SCALABILITY ISSUES

5.2.1 Extensive Requirements Definition and Validation Is Required

Many would underestimate the system design impact of the legal compliance requirements, the variance in election official processes, and the requirements established by the state certification bodies. Election administration needs vary, not just from state to state, but from county to county as a result of demographics and other factors.

For future initiatives, the associated requirements analysis and validation would need to be as rigorous and comprehensive as that done for the VOI Pilot. The complexity of the requirements analysis effort will grow very quickly as the system scales to accommodate a larger percentage of the UOCAVA population. The analysis will need to consider many factors in each jurisdiction including functional, legal, and workflow factors for the remote registration and voting system as well as existing LEO systems.

5.2.2 Distribution of Digital Certificates for Non-DoD UOCAVA Citizens Must Be Considered

One of the benefits of using the DoD PKI for the VOI Pilot is that the DoD had a certificate distribution infrastructure in place. This evolving infrastructure provides for the distribution of certificates at no cost to the individuals receiving them. However, the DoD PKI will distribute certificates only to active duty military, their dependents, DoD employees, and selected other personnel associated with the DoD, but not to the other population segments covered under UOCAVA. Clearly, the distribution of digital certificates to the other UOCAVA segments must be addressed in a larger scale system.

Currently, several Federal and state government efforts are underway to allow commercial PKIs to interface with the DoD PKI. This would in turn allow non-DoD UOCAVA citizens to receive digital certificates that are interoperable with the DoD PKI. These technical efforts hold promise for having a PKI system available for use by most, if not all, non-DoD UOCAVA citizens. However, these efforts only address the technology dimension of this issue.

A second issue associated with providing non-DoD UOCAVA citizens with digital certificates is the question of cost and accessibility. The availability of technology does not mean that it is accessible to citizens nor does it address the question of who pays for the digital certificate. Although the answer to these questions is unknown at this time, various states (e.g., Utah, Minnesota, Illinois) and Federal agencies (e.g., General Services Administration, United States Postal Service) are moving forward with digital signature legislation and/or a PKI program that will eventually permit any citizen to obtain and use a digital certificate. One of the often cited uses for these certificates is to facilitate citizen participation in future Federal and state E-Government programs, of which remote registration and voting can be a part.

For future initiatives, any remote registration and voting system would need to be interoperable with the DoD PKI as well as other Federal, state, and commercial PKIs. Also, acceptable protocols would need to be established for the distribution of these commercial certificates.

5.2.3 Broader Integration With Current LEO Equipment and Processes Is Required

To accurately evaluate the effectiveness of the VOI security architecture, the system was designed to operate independently of other LEO automated systems. By excluding automated interfaces, security challenges introduced from interconnected systems were eliminated. Although this proved beneficial to validate the security architecture, it generated an additional burden for the LEOs.

For future initiatives, there are several areas where additional system functionality would be required by a larger scale Internet voting system. Further, the additional functionality would need to be integrated with other existing automated systems in use by the local election office. The following subsections address four essential capabilities that would need to be developed and integrated with the existing registration and voting infrastructure at the LEO. The extent to which this can be done will be an important factor in determining whether any cost savings or cost burdens will be associated with a remote registration and voting system.

E-Ballot Generation in the Pilot Was a Duplicative Activity

The Pilot LEOs were required to create two ballots: one for the standard by-mail process and an electronic ballot for the VOI Pilot. Because the VOI E-Ballot Tool was separate from the by-mail ballot generation tools and process, the LEOs had to perform similar ballot creation activities twice. Although this duplicative activity was acceptable for the small number of citizens participating in the Pilot, this would not be the case for a larger scale system with thousands of citizens. For future initiatives, LEOs will need a ballot creation capability that will allow them to design and generate both by-mail ballots and E-Ballots without duplication of effort.

Automatic Mapping of the Citizen Address to the Appropriate E-Ballot Style Is Necessary

During the EFPCA approval process, the LEOs were required to print out the registration data received at the LEO servers and consult their existing registration databases to determine whether the citizen was eligible to vote absentee in their jurisdiction. Although this manual interface was acceptable for the small number of citizens participating in the Pilot, this would not be the case for a larger scale system involving thousands of citizens.

As noted during discussions with state certification officials, it is important to minimize those instances that require a person to re-enter data into one system that already exists in another system. Avoiding these types of manual processes eliminates the possibility for human error. For future initiatives, the system would need to automatically exchange data with the existing registration database or other LEO systems for a quick and seamless review of EFPCAs and the associated assignment of either a precinct or a ballot style to the citizen.

Automatic Interface Between Ballot Processing Tools and Tabulation Tools is Necessary

For the VOI Pilot, LEOs were required to print the E-Ballots before they could be tabulated. The printed E-Ballots were then manually transcribed to blank absentee ballots which could be counted by standard tabulation methods. This process proved very time consuming for the LEOs at the most demanding time in the election process. For a larger scale system, this process would not be feasible. For future initiatives, the remote voting system would need to provide either the choices from each ballot to an external tabulation subsystem via an electronic interface or be capable of performing tabulation itself.

Addition of an Automated E-Mail Generation Capability Would be Valuable

In those instances when an EFPCA is received by the LEO with incorrect data, such as a wrong address, the LEO needs to communicate those problems to the citizen. For future initiatives, the addition of an automated e-mail generation and transmission capability would provide for quick and error-free communication of that message. This capability would automatically generate an e-mail (partially or entirely) informing the citizen of the specific problem(s) and a recommended course of action to amend his/her application.

5.2.4 Legislation Supporting the Use of Remote Registration and Voting Via the Internet Is in the Early Stages of Development

Although a number of states have enacted legislation authorizing some form of electronic transmission of some election materials for UOCAVA absentee voters, Montana is the only state that has enacted legislation explicitly authorizing remote voting via the Internet. While legal authorization for remote Internet voting can be inferred from existing legislation in some states, ideally each state would pass legislation explicitly authorizing this alternative to the by-mail process.

Furthermore, although existing laws in some states can be interpreted to authorize the use of digital signatures as a legal substitute for a written signature on election materials, ideally each state would pass legislation explicitly authorizing the use of digital signatures in lieu of witnessed or notarized handwritten signatures for registration and voting materials.

5.2.5 The Model for Statewide Participation in UOCAVA Remote Registration and Voting Via the Internet Must Be Further Investigated

South Carolina participated in the VOI Pilot on a statewide basis. The LEO server was located in the state election office and the state election officials contacted the appropriate LEO via telephone, e-mail, and fax when election materials needed to be processed. This model would not be feasible when scaled to include thousands of UOCAVA citizens. For future initiatives, the remote registration and/or voting system would need to provide for the electronic exchange and access to registration information from geographically diverse locations within a state. Further investigation will be required on how to effectively administer elections via a computer network on a statewide basis.

5.2.6 Establishment of the Strategic Intent and Evaluation Criteria for the Pilot as First Steps Strengthens an Assessment

Technology proof-of-concept projects often focus on validating the effectiveness of the technical solution and pay limited attention to designing the project to evaluate the economic benefit or the effect of technology insertion on existing processes and participants. Evaluation criteria and strategic intent should be determined in the conceptual phase of a project to enable a systematic and thorough data collection and analysis from beginning to end. In the case of the VOI Pilot, the evaluation framework was established well into the implementation phase which resulted in some lost opportunities for data collection.

5.3 TECHNOLOGY RELATED LESSONS AND SCALABILITY ISSUES

5.3.1 The DoD PKI Brought Benefits and Challenges to the VOI Project

Although DoD PKI provided a strong identification and authentication framework for the VOI System, it also proved to be the greatest source of challenges for the Pilot. Some of these included—

- The DoD Medium Assurance PKI digital certificate distribution network was evolving and not as well established as originally projected. As a result, the FVAP personnel had to become certified as Local Registration Authorities to issue certificates to Pilot participants.

- Early versions of the DoD PKI documentation were confusing and sometimes incorrect, which caused difficulties for Pilot participants when they downloaded their certificates from the DoD PKI servers. The DoD PKI has migrated to a new version with revised documentation.

- The U.S. public is unfamiliar with digital certificates, which made its use a frustrating learning experience for most citizens.

- Participants had difficulty remembering their digital certificate passwords. Consequently, many certificates had to be reissued.

For future initiatives, not only would a more mature DoD PKI system be required, but it would also be beneficial if those certificates were being used by citizens for other applications. That would provide some degree of assurance that many UOCAVA citizens would have greater familiarity with this technology.

5.3.2 The FVAP Server Functionality Was a Key Architectural Feature

At the inception of the VOI Pilot, the FVAP server was conceived to operate in a manner analogous to how the FVAP office executes its mission by communicating between the citizens and the LEOs. By the conclusion of the System design, the FVAP server had been assigned the following responsibilities—

- Served as the single point of entry for all data requests and activities on the System. This proved valuable in that this single point of entry design increased the security of the entire System.

- Served as the single System component to interact with the DoD PKI and thus simplified the LEO server functionality and LEO workload.

- Provided for the strong identification and authentication of citizens in conjunction with the DoD PKI.

- Served as a trusted third party in performing electronic "postmarking" (inclusion of a time stamp), communication link verification, and System alarm capability.

- Provided a comprehensive audit trail of System transactions while preserving confidentiality of citizen information and ballot choices.

The strength and benefits of the FVAP server were commented on by several independent reviewers and it was noted as a powerful architectural construct within the VOI System. For future initiatives, it is clear that a centrally positioned server would need to be implemented in a manner very similar to that of the VOI System's FVAP server.

5.3.3 Creation of the E-Ballot Tool Proved Essential to System Success

The E-Ballot Tool became essential to the creation of E-Ballots and to the general success of the Pilot as a whole. The initial plan called for the development of an "E-Ballot Format Specification" and for the LEO staff to develop their E-Ballots via the use of a Hypertext Markup Language (HTML) editor. As a risk mitigation measure, the E-Ballot Tool was developed to minimize the chance that a subtle HTML format mistake made by the LEO staff would not be detected until the E-Ballots were being provided to Pilot participants. There was also some concern that HTML knowledgeable staff would not be available. An unanticipated benefit of the E-Ballot Tool became evident in responding to the requirements that undervoting and overvoting be detected by the VOI System and that bilingual E-Ballots be provided. The solution involved both subtle and precise changes to the E-Ballot's format specification. The manual inclusion of those HTML features by LEO staff would have further complicated their E-Ballot creation activities and increased the chance for human error. Although the LEOs thought that the entry of ballot information into two systems was a burden, all felt that the E-Ballot Tool was flexible enough to meet their diverse needs.

5.3.4 Security at the Citizen's Workstation Is One of the Key Challenges for a Remote Registration and Voting System

Use of home computers represents one of the greatest challenges for the large-scale deployment of an Internet registration and voting system. For the VOI Pilot, security at the citizen workstation was considered a minor issue. The limited scope of the project, limited distribution of the plug-in application, and limited publicity all combined to limit the degree of risk to the project. For that reason, the Pilot did not focus on the citizen workstation security issues. In a future scaled remote Internet registration and voting system, citizen workstation security will have to be considered in much greater detail. The VOI Peer Review Group, the *California*

Internet Voting Task Force Report, and the Internet Policy Institute *Report of the National Workshop on Internet Voting: Issues and Research Agenda* all caution against the use of remote voting systems based on security threats present at the citizen workstation (principally malicious software) and existing or new threats against the integrity of elections as a result of using the Internet.

In support of future initiatives, a security risk assessment and management perspective should be taken to frame the specific issues that exist as a result of using the Internet to support remote voting. Ultimately, it will be important for technologists to frame a meaningful discussion on the existing security risks, available countermeasures, and the resultant residual security risk (i.e., the risks that still exist after applying countermeasures). Arising out of these discussions will be a better understanding of this complex landscape and a plan for addressing remaining risks. The products required from this discussion are technical guidance and requirements that can be used to help establish new Internet voting standards. Once this topic is examined and discussed in the technical and standards development communities, state and local election officials, citizens, and other interested parties will be in a much better position to make an informed decision on the future of Internet voting for a broad-scale citizenry.

5.3.5 A Larger Scale Pilot Will Result in More Visibility and Potentially Attract Those With Malicious Intent

The VOI Pilot was not highly publicized. This may have provided some protection from security threats that would not be available with a larger scaled, more visible system. A larger scale effort would focus attention on the system, potentially making it an attractive target for malicious hackers or others who might want to affect an election's outcome.

Although this type of malicious activity has the potential of being a "showstopper," no architectural, design, or implementation security defect was uncovered during the Pilot. Although any future system would minimally incorporate the security features demonstrated in the Pilot, it is important to note that system security is not a static condition. Vulnerabilities in commercial hardware and software are discovered and exposed on a regular basis. The key to security is constant diligence, which includes not only the monitoring of vendor and hacker sites for exposed vulnerabilities but also the continuous monitoring of the system and the careful review of security logs.

For future initiatives, industry best practices would be implemented for the system, including a rigorous implementation of constant diligence. Additional practices might include independent third party, "white hat" hacking efforts directed at test systems to discover system specific vulnerabilities. Security would remain a high operational priority.

5.3.6 Breadth and Depth of System Certification Activities Were Significant

For the Pilot, considerable attention was expended in the area of certification and accreditation. For this project, two complementary and required certification and accreditation efforts were undertaken. The first was associated with the DoD system certification and accreditation process, whereas the second activity was associated with the System receiving certification for use in the State of Florida.

Adding to the amount of effort and time required for these activities was the lack of existing state or Federal standards for Internet registration and voting. The project team worked with State of Florida officials to tailor existing Florida standards and procedures for application to an Internet-based voting system. The DoD certification test procedures were used as part of this process.

Another important challenge was ensuring the independent testing team was well informed of the system requirements, design, and implementation. This effort required a significant investment on the part of highly skilled testers to attain a level of expertise that permitted them to develop well-conceived test procedures. Because interface and functional testing standards were not available to the third-party testers, they were required to research many internal and design details that required much time and technical expertise.

Clearly, Internet voting standards must be developed to allow the further use of Internet voting systems. The results and products from this Pilot should be incorporated into ongoing voting system standards development efforts under the Federal Election Commission.

5.3.7 Software Sent to the Citizens Via the Postal Service Is Less Time Effective than Electronic Delivery

The delivery of VOI software on CD-ROM via commercial carriers, domestic and international postal services to the participating citizens was time consuming. In a scaled system, mailing documentation would be more time consuming and very costly. In the future, use of the Internet for posting system documentation and software would be a more efficient option.

5.3.8 More Robust Server Sites Are Required

The FVAP server was the single point of entry for the VOI System; it was unavailable for short periods several times during the Pilot. The individual LEO servers also experienced several outages, mostly related to telecommunications connectivity external to the VOI System. One LEO server went down temporarily on election night but was restored to service and the voter successfully resubmitted his/her ballot. Since the VOI System was a small proof of concept pilot, it was not implemented with the degree of robustness that would be needed for a large scale system.

When a citizen was attempting to access the System during a LEO server outage, that person was contacted by phone or e-mail and asked to resubmit his/her transaction after the server was back in operation. In a larger-scale system, this approach would not be feasible. It would also run the risk of undermining public confidence in the system, discouraging use by the citizens. A larger-scale system would require that all server sites be much more robust similar to current high-end commercial Web sites. Requirements to ensure greater availability would include—

- Redundant parallel servers and separation of duties (i.e., separate Web and database servers)

- Backup power sources that could run the system for extended periods of time

- Geographically separate backup servers in case of physical damage to LEO and/or FVAP facilities

- Alarms (e.g., pages, instant online messages) for LEOs so they are immediately aware when an error condition occurs

- Redundant network paths (e.g., Internet Protocol addresses, Internet Service Providers).

6.0 DISCUSSION AND RECOMMENDATION

This section presents a discussion of alternatives and FVAP's recommendation for further steps in examining the feasibility of using the Internet for remote UOCAVA registration and voting. Section 6.1 contains the framework for the development of the alternatives considered, based on the positive and negative attributes of the VOI Pilot System. Section 6.2 contains a discussion and analysis of the alternatives. Section 6.3 presents the multistep recommendation and its rationale. Section 6.4 provides a conclusion.

6.1 DISCUSSION FRAMEWORK

To provide a basis for understanding the candidate systems considered and how the recommended system was selected, it is useful to summarize the registration and voting activities that the VOI Pilot System provided. Figure 6.1-1 provides an overview of those activities, organized into three categories: registration, status checking, and voting.

Figure 6.1-1. VOI Pilot System Activities
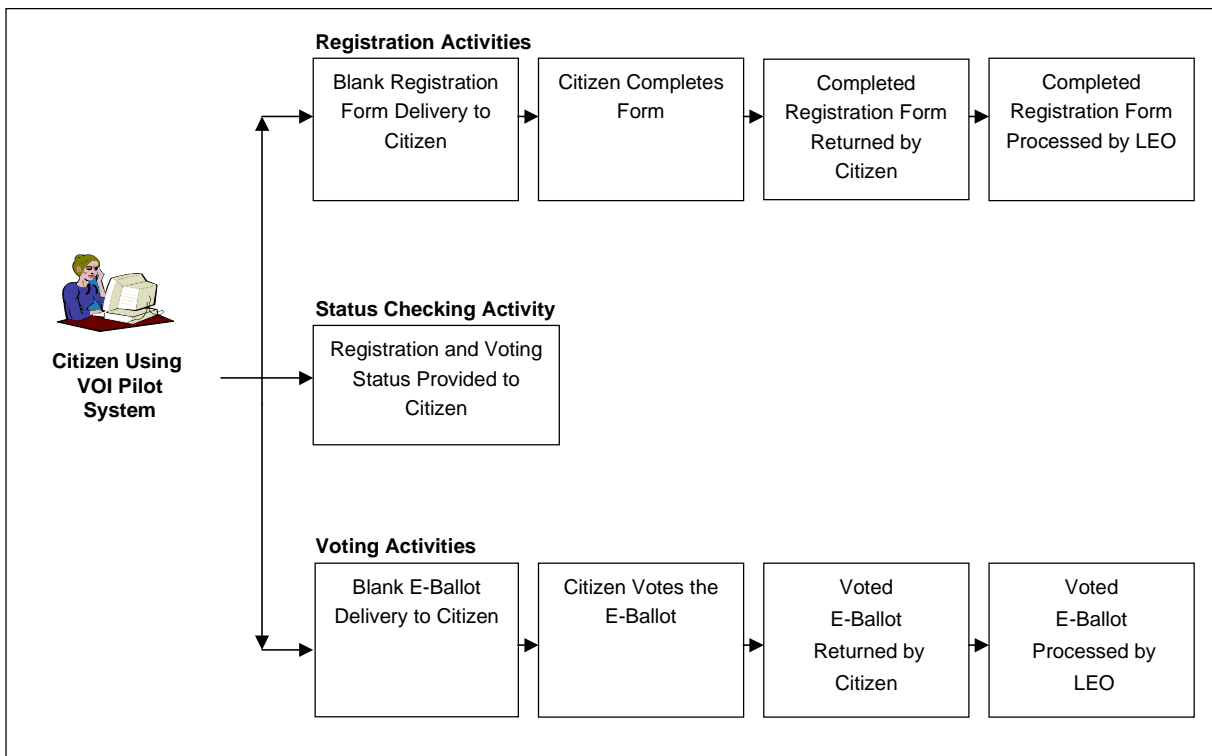
Registration is the first activity performed by the citizen, whereas voting occurs at the end of the cycle. Under the current provisions in many states, UOCAVA citizens may submit an absentee registration and ballot request application in January of each year. If approved, this application qualifies the citizen to receive an absentee ballot for all elections in that year for which he/she is eligible to vote. Some states require an application for the primary, general, run-off, or special elections in the year; others accept the application at different time periods. The citizen can invoke status checking at any time during the registration and voting time period. The following

paragraphs provide an overview of how the VOI Pilot System performed each activity and highlight the positive and negative attributes of this approach.

6.1.1 Registration Activities[17]

Blank Registration Form Delivery

The citizen logs on to the VOI System, identifies his/her local election office, and requests an Electronic Federal Post Card Application (EFPCA). The VOI System downloads the EFPCA via the Internet to the citizen's local workstation.

Positive Attributes	• Provides strong identification and authentication of the citizen • Provides instant delivery of the EFPCA to the citizen • Provides an EFPCA tailored to the data requirements of the citizen's state • Allows update of registration data through submission of a new EFPCA
Negative Attributes	• Partial update of registration data requires completing and submitting a replacement EFPCA

Citizen Completes Form

The citizen fills out the form in accordance with the instructions provided.

Positive Attributes	• Eliminates the by-mail problem of illegible forms • Ensures that all forms are complete • Allows updating of address or other information, as required • Includes all instructions online with the form
Negative Attributes	• None

Citizen Submits Completed Registration Form

After completing the EFPCA, the citizen uses his/her digital certificate to sign the form. The local workstation sends the completed and signed form to the local election office via the Internet.

Positive Attributes	• Provides strong identification and authentication of the citizen • Ensures that all forms are signed • Provides instant delivery of EFPCA to the local election office • Provides citizen instant confirmation that EFPCA was received
Negative Attributes	• None

LEO Processes Registration Form

After receipt of the completed and signed form at the local election office, the election official reviews the form's content to establish whether this person is eligible to vote absentee in that

---

17 Workstation viruses, malicious code, and denial of service attacks are always a consideration when using the Internet. These are not shown as negative attributes for any registration activities for several reasons. The content of the registration form is reviewed by the LEO who can identify anomalies. The citizen can verify his/her status and contact the LEO if something seems out of order. Except when the filing deadline is imminent, registration activities are not time-sensitive, so denial of service is not a significant concern.

jurisdiction. The LEO may print the form from the VOI System to facilitate verification of the data with the local voter registration database. If the form is approved, the LEO assigns a jurisdictional identifier or a ballot style type to the citizen and records this information in the LEO's voter registration database and in the VOI System. The citizen's status information is automatically changed based on whether his/her form was approved or denied by the LEO.

Positive Attributes	• System captures all LEO EFPCA transactions for ease of processing and workload management • System automatically updates citizen status information when the LEO processes the EFPCA
Negative Attributes	• LEO has to communicate "out of band"[18] with citizen if there are any questions about his/her application • There is no automated interface between VOI System and local voter registration database • Jurisdictional identifier/ballot type must be manually entered into VOI System

6.1.2 Status Checking Activity

Citizen Checks Status

The citizen logs on to the VOI System, identifies the local election office, and requests his/her current registration or voting status. The VOI System downloads a status message via the Internet to the citizen's workstation. Any action the LEO takes in regard to a citizen's application causes the status information to be automatically updated.

Positive Attributes	• Provides strong identification and authentication of the citizen • Provides instant feedback to the citizen at any location
Negative Attributes	• Citizen cannot verify the accuracy of his/her submitted registration information as recorded in the voter registration database • Citizen cannot communicate with LEO through VOI System

6.1.3 Voting Activities

VOI System Delivers Blank Ballot

The citizen logs on to the VOI System, identifies the local election office, and requests his/her electronic ballot (E-Ballot). The VOI System downloads the E-Ballot via the Internet to the citizen's local workstation. The citizen can print the ballot to use as a sample ballot or can vote the ballot.

Positive Attributes	• Provides strong identification and authentication of the citizen • Provides instant delivery of the blank ballot to the citizen at any location • Citizen does not need to go to mail room or other location to get his/her ballot • Provides opportunity for citizen to review ballot before voting
Negative Attributes	• Internet denial of service attack may prevent downloading of ballot

---

18 The VOI System did not have an integrated e-mail capability, therefore the LEO had to use another system to contact citizens.

Citizen Votes E-Ballot

The citizen uses the mouse and keyboard to indicate selections on the E-Ballot. He/she can also enter write-in candidates via the keyboard, if required. If the LEO has elected to activate this feature, the citizen will be advised if he/she has overvoted or undervoted a race on the ballot.

Positive Attributes	• Voter selections are clear and unambiguous • Approach provides opportunity for citizen to correct unintentional overvote or undervote
Negative Attributes	• There is a possibility of malicious software operating at the citizen workstation that would affect the voted ballot

Citizen Submits Completed Ballot

After the citizen votes the E-Ballot, he/she uses the digital certificate to sign the ballot. The local workstation encrypts the E-Ballot, then sends the voted, encrypted, and signed ballot to the citizen's local election office via the Internet.

Positive Attributes	• Provides strong identification and authentication of the citizen • Delivers the voted ballot instantly to the appropriate local election office • Provides instant confirmation to the citizen that the voted ballot was received • Ballot "postmarked" by FVAP server
Negative Attributes	• Internet denial of service attacks may prevent submission of voted E-Ballot • FVAP and LEO servers may be susceptible to hacking attempts • Possibility of malicious software operating at the citizen workstation that would affect the voted ballot

6.1.4 LEO Processes Ballots at Local Election Office

After receipt of the voted, encrypted, and signed E-Ballot at the local election office, the ballots are stored in encrypted form on the LEO server until the designated time for ballot processing. At that time, the election officials reconcile the E-Ballots received and validate those that will be counted. Two people are required to initiate and control the process that removes the voters' identities from the ballots for confidentiality, decrypts the contents, and prints the ballots. Each citizen's status information is automatically changed based on the processing that has occurred. The printed ballots are then transcribed to paper ballots that can be entered into the LEO's tabulation system.

| Positive Attributes	• Approach reduces the possibility of ballot tampering because the ballots are in a secured, encrypted file under two-person control and subject to "one-person, one-vote" validation • The ballots are encrypted until the voters' identities are removed, making it impossible to determine how particular citizens voted
Negative Attributes	• Time needed to print ballots was lengthy and occurred at the most time-sensitive point of the election process • Printed ballots must be manually transcribed for tabulation, which is very time consuming and may introduce human error

6.2 DISCUSSION AND ANALYSIS OF ALTERNATIVES

Based on the results and lessons learned from the VOI Pilot effort, the FVAP has identified four alternative system concepts for consideration as a follow-on pilot system. These alternatives address a broad set of operational capabilities that might be provided to UOCAVA citizens in the future.

6.2.1 Remote Registration and Status Checking Alternative

This system (illustrated in Figure 6.2-1) allows a citizen to remotely register to vote, check status, review his/her registration data, and update registration information, as needed. For initial registration, the citizen would request and submit an EFPCA form. For updating registration information, he/she would select the Update Registration option. These capabilities would be integrated with the LEO's voter registration system. With this integrated system, the approved EFPCA table would provide the LEO with a listing of citizens and mailing addresses. Citizens would receive and return their absentee ballots by mail. The Check Status capability would be expanded to include when the ballot was mailed by the LEO and when the LEO received the returned voted ballot. The Check Status capability would also allow the citizen to verify that all registration data submitted were properly recorded. An integrated e-mail capability would facilitate quick and easy communications between citizens and LEOs.

Figure 6.2-1. Remote Registration and Status Checking System Activities
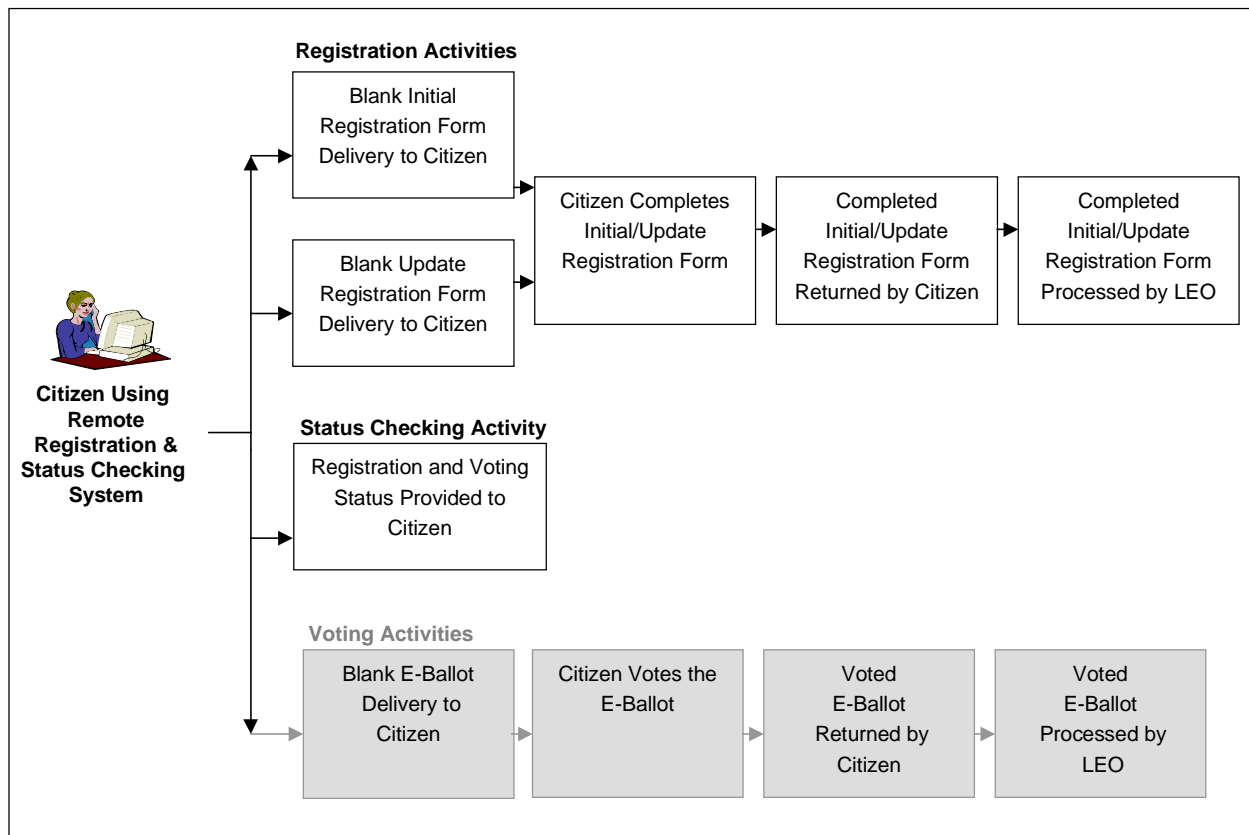
Analysis of Remote Registration and Status Checking Alternative

This alternative provides all of the registration and status checking functional capabilities. It adds an Update Registration capability that would allow updating of a portion of registration information without requiring the citizen to complete and submit a replacement EFPCA. A benefit of this capability is that it allows the citizen to easily and quickly update his/her mailing address if he/she has relocated between the time of the initial registration application and the time ballots are due to be mailed (a key UOCAVA citizen and LEO concern). In addition, military voters who are on short-term deployment from their home base could provide a temporary address so their ballots could be sent to their deployed location instead of to their home base mailing address. This capability should considerably mitigate the problems of mailed ballots being returned as undeliverable or not reaching temporarily deployed personnel in a timely manner. This function, combined with an embedded e-mail capability, has the potential to save considerable LEO time and effort in keeping the data in the voter registration database current. This would also reduce the FVAP time and effort spent in querying the Defense Manpower Data Center database to verify duty status and to update mailing addresses in response to LEO requests.

This alternative does not directly support any of the remote Internet voting capabilities. The citizen would still receive his/her ballot by mail, vote it by hand, and return it by mail. However, this alternative does have several features that are expected to significantly improve the successful and timely delivery of by-mail ballots. The Update Registration capability would allow citizens to easily update their mailing addresses, including adding a temporary address, which should reduce the number of undeliverable or late-received ballots. In addition, the LEO could enter the date when the ballot was mailed in the citizen's status information. The citizen could log on to the Check Status function and have some idea of when the ballot might arrive. The citizen could also send an e-mail to the LEO when he/she puts the voted ballot in return mail, and the LEO could post the date when the ballot was received. These capabilities would allow both the LEO and the citizen to monitor the by-mail ballot process and provide an opportunity to timely address any problems that might arise. In addition to these improvements, this alternative avoids the security risks associated with sending ballots via the Internet and the malicious code risk at the citizen workstation. It also provides a significant improvement over the by-mail FPCA in the degree of assurance provided regarding the identity of the citizen.

Positive Attributes	• Provides strong identification and authentication of the citizen • Provides instant delivery of the EFPCA to the citizen • Provides an EFPCA tailored to the data requirements of the citizen's state • Includes all instructions online with form • Allows updating of address or other registration data through submission of an update form • Eliminates the by-mail problem of illegible forms • Ensures that all forms are complete • Ensures that all forms are signed • Provides instant delivery of EFPCA to the local election office • Provides citizen instant confirmation that the EFPCA was received • System captures all EFPCA transactions for ease of processing and workload management by the LEO • System automatically updates citizen status information when the LEO processes the EFPCA • LEO can communicate through system with citizen if there are any questions about his/her application • Automated interface between VOI System and local voter registration database • Jurisdictional identifier/ballot type automatically assigned • Provides instant status feedback to the citizen at any location • Citizen can verify the accuracy of his/her submitted registration information as recorded in the voter registration database • Citizen can communicate with LEO through VOI System • Notice of LEO ballot mailing date in Check Status • E-mail to LEO from citizen when ballot put in return mail
Negative Attributes	• Internet denial-of-service attacks may cause delay • FVAP and LEO servers may be susceptible to hacking attempts that would disrupt operations • Possibility of malicious software operating at the citizen workstation that would affect the registration form

6.2.2 Print and Mail Alternative

This system (illustrated in Figure 6.2-2) builds on the capabilities of the Remote Registration and Status Checking alternative by adding the capability of delivering an E-Ballot to the citizen. When the E-Ballots are available, this information is accessible via the Status Check feature. The citizen downloads the ballot to his/her workstation and votes it online. The citizen would then print the ballot in machine-readable format and mail it back to the LEO. The printed ballot would include each citizen's digital certificate information for authentication purposes, as well as a locally generated time stamp. The citizen could e-mail the LEO with the date that he/she mailed the ballot. When the ballot is received, the LEO can post the date of receipt so that the voter can verify through the Status Check capability when his/her ballot was delivered.

Figure 6.2-2. Print and Mail System Activities
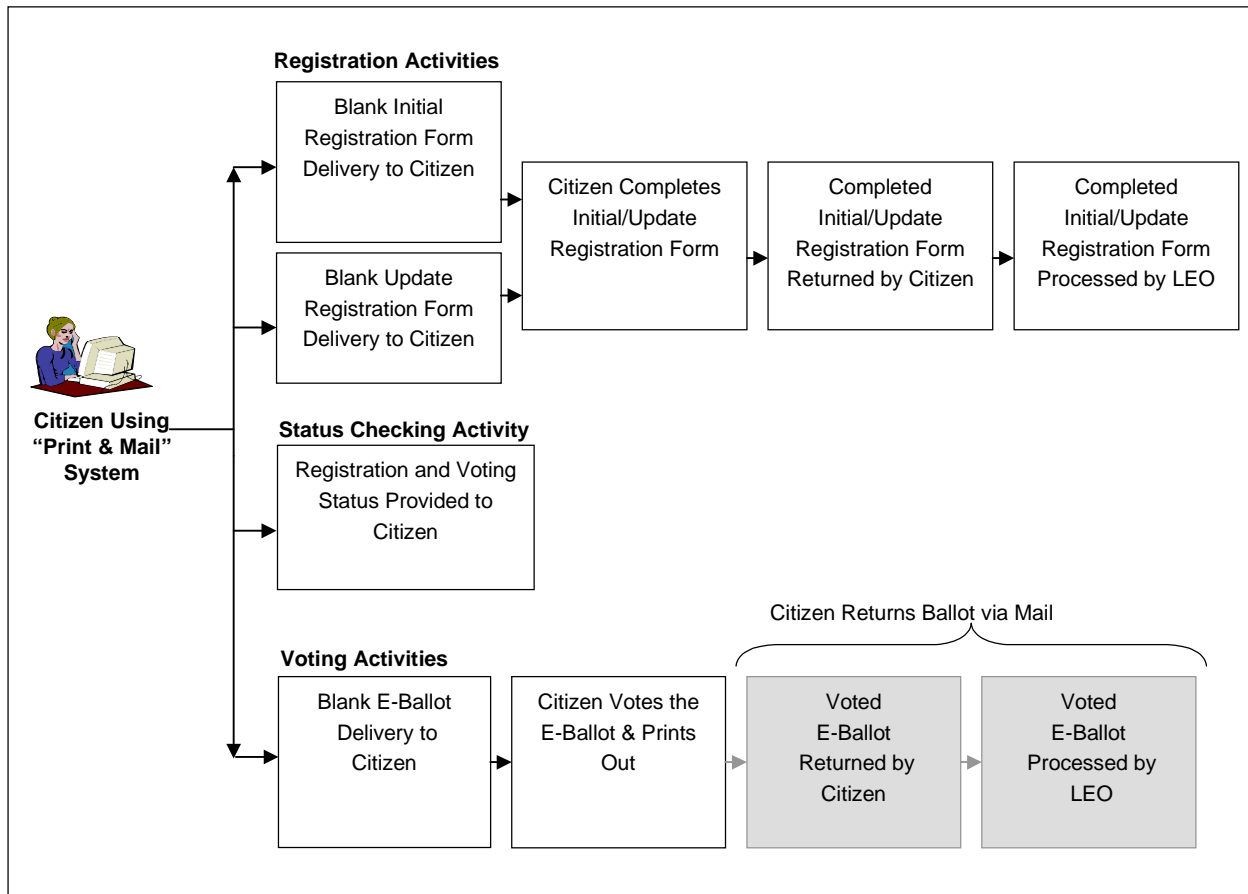
Analysis of Print and Mail Alternative

This alternative provides all of the required functional capabilities except for electronic return of the ballot. Internet delivery of the ballot eliminates the by-mail transit time to the citizen. The LEO can determine from the system audit log when the citizen downloaded the ballot to verify when he/she actually received it. If the citizen e-mails the LEO with the date he/she put the ballot in the return mail, the LEO will know approximately when the ballot might be received. This approach provides positive authentication of voter identity by automatically printing his/her digital certificate identifier on the ballot. By allowing the citizen to vote the ballot on his/her workstation, it ensures that all ballot choices are clear and that the digital signature is applied. It could also provide an undervoting and overvoting notice to the citizen to ensure that all choices are validly marked and can be properly counted.

There are at least two significant technical unknowns with this alternative. The first is the question of whether an acceptable quality machine-readable ballot could be printed at the citizen's workstation, given the tremendous number of different printers in use and the variable status of equipment maintenance. The second is whether a machine-readable format could be input directly into the LEO's tabulation system or if an intermediate processing step would be required. With the additional benefits of eliminating half of the ballot transit time and the improved quality of ballot marking, this alternative offers significant advantages over the
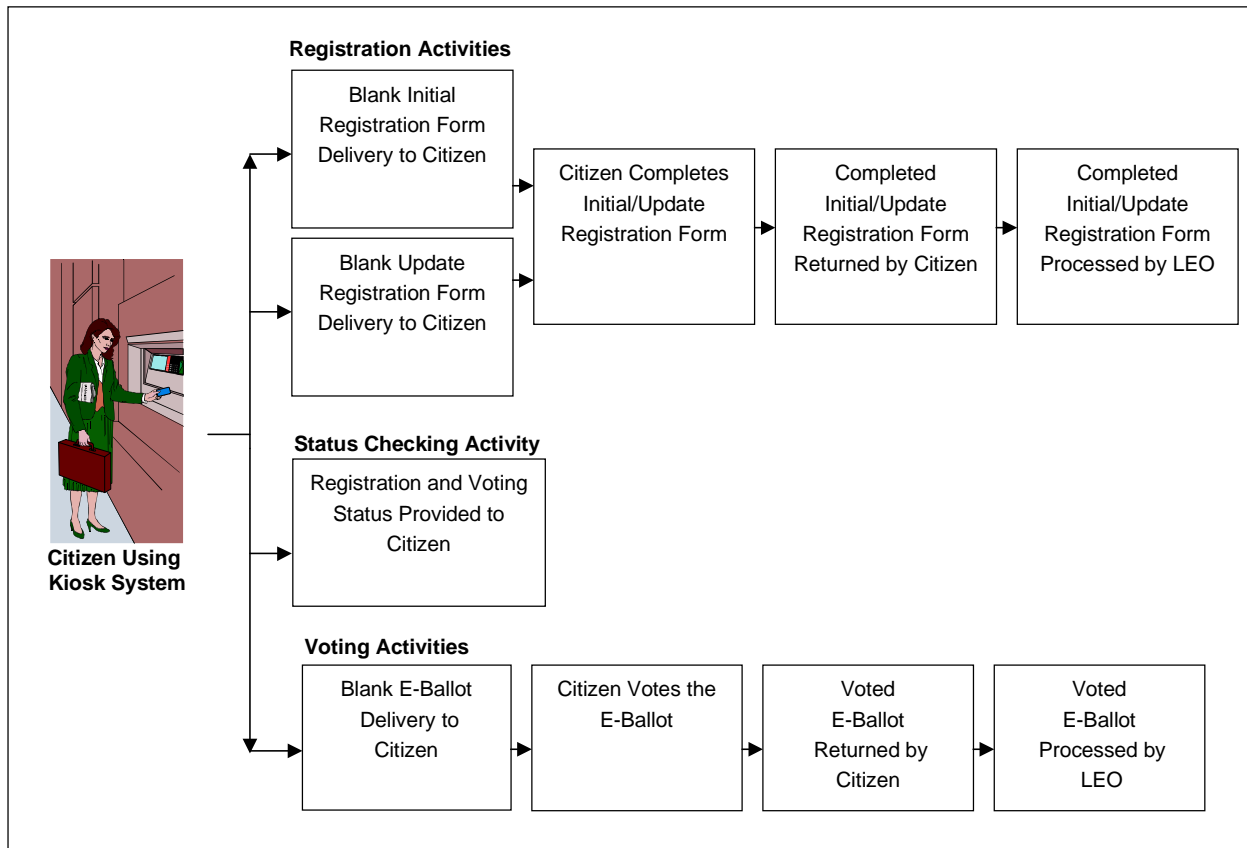
Remote Registration and Status Checking alternative. However, in-depth analysis is needed to determine the technical feasibility of this approach.

Positive Attributes	• Notification to voter when ballot available through Check Status • Voter selections are clear and unambiguous • Provides opportunity for citizen to correct unintentional overvote or undervote • Provides instant delivery of the blank ballot to the citizen at any location • Citizen does not need to go to mail room or other location to get his/her ballot • Provides opportunity for citizen to review ballot before voting • LEO can verify when citizen downloads document • Positive voter identity on ballot by printing certificate data
Negative Attributes	• Technical feasibility research is required • Quality of printed ballot from citizen printer • May require interim processing by LEO before tabulation • Internet denial of service attack may prevent downloading of ballot • Possibility of malicious software operating at citizen workstation that would affect the ballot • Citizen has to pay postage • Citizen has to correctly package in privacy envelope • Citizen has to get correct return address on envelope

6.2.3 Kiosk Alternative

This system (illustrated in Figure 6.2-3) would allow a citizen to register, vote, and check his/her status via the Internet with similar functionality to the VOI Pilot System. It would also incorporate the features from the Remote Registration and Status Checking alternative. The principal difference in this alternative is that the citizen would be required to use a specially designated and controlled workstation (kiosk) instead of his/her personal or work computer. This is a solution for secure Internet voting that has been proposed for use in the U.S.

Figure 6.2-3. Kiosk System Activities

Analysis of Kiosk Alternative

This alternative provides all the remote registration, status checking, and voting capabilities. In this alternative, the individual citizen workstations would be replaced by a network of dedicated computers (kiosks) deployed throughout the world. In the VOI Pilot System, the citizen's workstation was outside the security perimeter of the system. In the kiosk system, the workstation would be within the security perimeter. This has the advantage of protecting against the introduction of malicious code into the System, which was a possible security risk identified for the citizen workstation in the VOI Pilot System. If the kiosks communicate with the LEOs through the Internet, they would still be subject to denial of service attacks.

Because UOCAVA voters are located all over the world, the logistical aspects associated with this approach are prohibitive. Providing kiosks for UOCAVA voters would require thousands of machines, with all the attendant issues of location, maintenance and security. Since the citizen would have to go to the kiosk location, it would not be a very convenient alternative compared with receiving voting materials at his/her location. It also might not be a very practical approach if the citizen must travel any great distance.

Positive Attributes	• Within security perimeter of the system, so no malicious software problem
Negative Attributes	• Complex logistics (1000s of kiosks, 1000s of locations) • Manning and maintenance expensive • Each kiosk would have to link to possibly hundreds of LEOs • Citizen would have to travel to get to kiosk • Subject to denial of service attack • FVAP and LEO servers may be susceptible to hacking attempts

6.2.4 Remote Voting Alternative

The remote voting system (illustrated in Figure 6.2-4) would provide all remote registration and voting functions from the citizen's workstation and would be very similar to the VOI Pilot System from the citizen's perspective. It would provide the additional functionality developed for the Remote Registration and Status Checking alternative. From the LEO's perspective, it would include interfaces with the local ballot creation and tabulation systems and thereby eliminate all manual interface processes.

Figure 6.2-4. Remote Voting System Activities
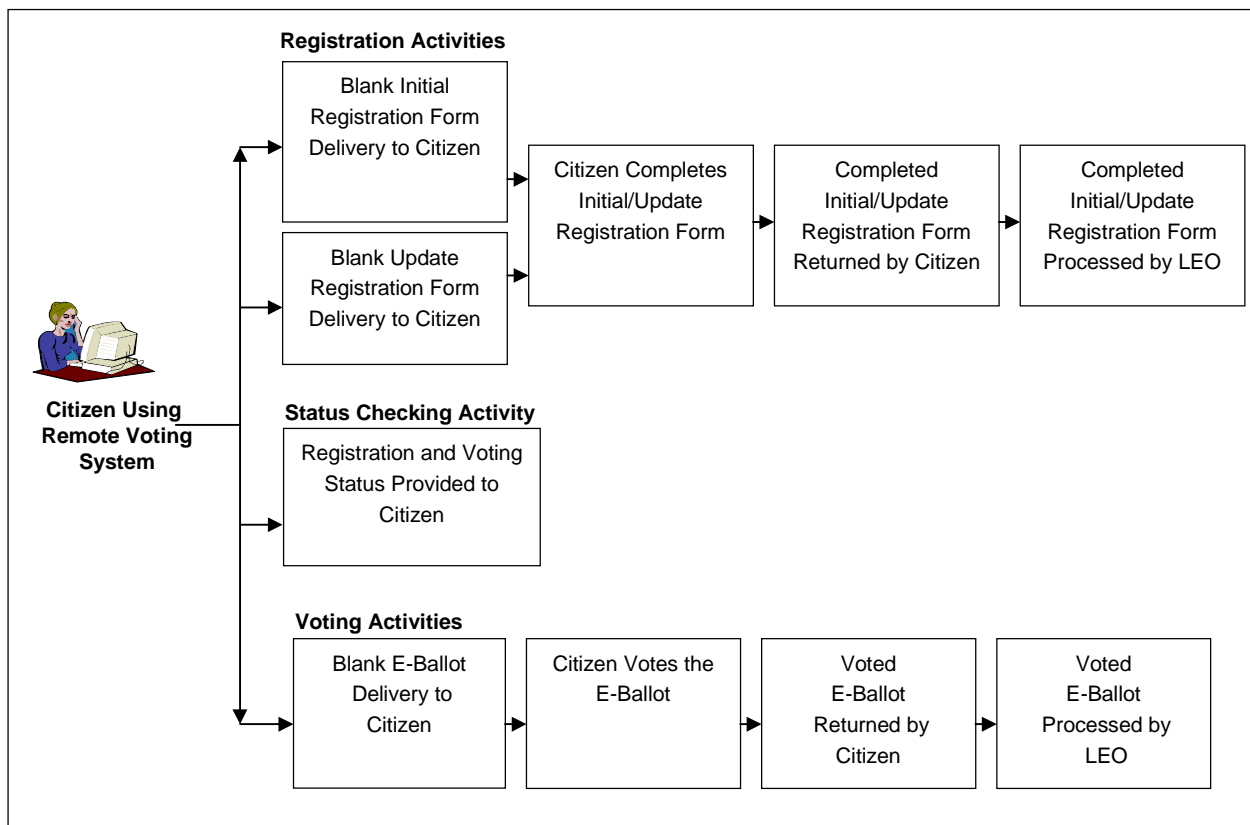
Analysis of Remote Voting Alternative

This alternative is subject to the same security concerns as the current VOI System. For this reason, we cannot recommend this alternative as an immediate follow-on development to the VOI Pilot. However, this alternative resolves nearly all the by-mail process problems and would

provide the greatest benefit for UOCAVA voters. Therefore, we recommend that research continue on these security issues so that this alternative could be implemented in the future when adequate security measures are available to counteract the malicious software (e.g., virus and Trojan Horse) threat and denial of service attempts.

Positive Attributes	• Delivers the voted ballot instantly to the appropriate local election office
	• Provides instant confirmation to the citizen that the voted ballot was received
	• Ballot "postmarked" by FVAP server
	• Approach reduces the possibility of ballot tampering because the ballots are in a secured, encrypted file under two-person control and subject to "1-person, 1-vote" validation
	• The ballots are encrypted until the voter's identities are removed, making it impossible to determine how particular citizens voted
Negative Attributes	• Internet denial of service may prevent download of blank ballot or submission of voted ballot
	• FVAP and LEO servers may be susceptible to hacking attempts
	• Possibility of malicious software operating at the citizen workstation that would affect the voted ballot

6.3   RECOMMENDATION

6.3.1 Recommendation Part 1

Implement a broader scale pilot project for remote registration and status checking that is electronically integrated with existing voter registration systems in one to three states for the 2004 General Election.

The VOI Pilot project was a feasibility study that demonstrated that a stand-alone system for remote registration and voting over the Internet can be a secure, viable alternative to the by-mail process in a small-scale, tightly controlled environment. However, there are a number of security concerns in expanding remote voting to a larger population at this time. These include the possibility of malicious software on citizen workstations and the susceptibility of Internet systems to denial of service attacks and hacking. There are also challenges in developing an optimized system that integrates well with LEO election administration workflow. While there is a high degree of commonality in LEO processing of UOCAVA forms, it is not a uniform process across all jurisdictions. A complex technical issue is that of providing an electronic interface with the multiplicity of existing voter registration systems. In addition, there are many unanswered questions regarding the affordability and supportability of this technology at the county level. For all these reasons, the FVAP recommends a next step that provides significant improvement to the UOCAVA by-mail process while minimizing the security risks inherent in today's Internet technology. A broader scale project would also provide a realistic operating environment in which to examine alternative implementation strategies and their impact on system affordability and supportability.

Table 6.3-1 lists common problems with FPCA forms identified by LEOs who responded to the 1996 FVAP Post Election Survey. The numbers indicate the percentage of LEOs who

experienced these problems. The Remote Registration and Status Checking alternative eliminates all of the problems listed in Table 6.3-1. This would save time and effort for the LEO and the citizen in getting sufficient and accurate information to determine the voter's eligibility to vote absentee. This alternative provides timely feedback to the citizen that his/her FPCA was received.

Table 6.3-1. FPCA Problems Eliminated by Recommended Remote Registration and Status Checking System

PROBLEM	ELIMINATED
No/Inadequate home address (66%)	✓
Inadequate/illegible mailing address (25%)	✓
Illegible writing (18%)	✓
Incomplete form (13%)	✓
No signature (11%)	✓
No witness signature/address (4%)	✓

Source: FVAP 1996 Post Election Survey Final Report

This alternative would also allow for easy updating of registration information, including the ability to provide a temporary address for those instances in which a military voter is deployed from his/her home base when ballots are mailed. This is expected to reduce the number of ballots returned as undeliverable and to improve the timely receipt of ballots by the UOCAVA voters. Providing additional information in the Check Status feature, such as when ballots were mailed out by the LEO and when the returned ballot was received, will enable the LEO and the citizen to better track ballot transit and enable more timely identification and resolution of possible problems. An integrated e-mail capability would allow quick communications between the LEO and the voter.

This alternative is less subject to the security concerns associated with the use of the Internet for voting. It provides considerable improvements over the by-mail process, which the FVAP believes would significantly enhance the successful participation of UOCAVA voters in the electoral process. This alternative also supplies a foundation that can easily be expanded to include additional voting-related functionality when adequate security safeguards become available to minimize risk on a broader scale.

6.3.2 Recommendation Part 2

Continue participation in the development of Internet registration and voting system standards.

The FVAP VOI Pilot Program has been on the leading edge of the development of certifiable Internet voting systems. As noted in Section 5, the lack of Internet voting system standards resulted in considerable additional effort to define reasonable standards against which the VOI Pilot System could be evaluated. Before any registration and voting system can be fielded for public use, the system will need to be tested and certified. Certification standards must be in place for these activities to be performed.

In support of this recommendation, the FVAP would assist various organizations in their standardization activities. Those organizations would include—

- Voting system standards organizations (e.g., Federal Election Commission)

- State certification bodies, as requested

- Federal and international technology standards organizations (e.g., National Institute of Standards and Technology, International Organization for Standardization)

- Commercial technology standards organizations (e.g., Internet Engineering Task Force).

6.3.3 Recommendation Part 3

Support state legislative initiatives to allow remote registration and voting.

Enabling legislation will need to be passed by state legislatures to support future pilot activities and the eventual operational use of this technology. The FVAP would work with state officials to promote enabling legislation to—

- Facilitate the acceptance of remote electronic registration as official voter registration

- Facilitate the adoption and/or expansion of digital signatures for voter registration and voting

- Facilitate the adoption of remote Internet voting for UOCAVA citizens.

6.3.4 Recommendation Part 4

Continue research to identify solutions to outstanding issues to permit the eventual implementation and operational use of a remote registration and voting system.

Evolving from a Remote Registration and Status Checking pilot system will require the acceptable resolution of many issues, some of which have not yet been clearly defined. This recommendation would define the issues that must be resolved before moving ahead with a system for remote voting over the Internet. The scope of issues includes technological (including security), legal, cost and LEO workflow considerations. The framing and discussion of these issues will require participation on the part of diverse organizations and disciplines.

6.4 CONCLUSION

Figure 6.4-1 illustrates an evolutionary approach of building upon the experience gained from the groundbreaking VOI Pilot. This strategy is based on the premise that a low-risk, incremental approach is the most prudent way to proceed when dealing with such a fundamental right as voting. As the VOI Pilot demonstrated, remote Internet registration and voting has much to offer UOCAVA citizens. However, it also has challenges and pitfalls that must be resolved before full-scale implementation is attempted. The realization of this recommendation would ensure a

judicious and methodical progression from the current by-mail process to a secure, easy-to-use, and expedient remote Internet registration and voting system for UOCAVA citizens in the future.

Figure 6.4-1. Recommended Evolution of UOCAVA Remote Internet Registration, Status Checking, and Voting

Effort	VOI Pilot *1998-2001*	Remote Registration & Status Checking Pilot *2001-2004*	Research-Driven Solution Pilot *Beyond 2004*
Activities	VOI Pilot System Development, Operational Use & Assessment	Remote Registration & Status Checking System Development, Operational Use & Assessment Involvement in Development of Internet Voting System Standards Support Legislative Initiatives with States Research Remaining Issues Toward Development of— • Print & Mail Internet Voting Capability • Remote Internet Voting Capability	Remote Print & Mail System Development, Operational Use & Assessment **OR** Remote Voting System Development, Operational Use & Assessment
Scope	Small Scale Project (15 Counties <100 Citizens)	Large Scale Project (30-120 Counties 10,000-150,000 Citizens)	Large Scale Project (30-120 Counties 10,000-150,000 Citizens)