Secure Electronic Registration and Voting Experiment

For Internal Use Only

SERVE™

Table of Contents

Sections

1: Introduction and Overview

The National Defense Authorization Act for Fiscal Year 2002, passed in December 2001, directed the Secretary of Defense to conduct an electronic voting demonstration for the 2002 general election. The purpose of this demonstration was to continue research begun by the Department of Defense (DoD) in 1997 to examine the potential of Internet technology to overcome the barriers to voting participation experienced by absentee Uniformed Services members and overseas citizens. The voting rights of these citizens are protected by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), which is administered by the Director, Federal Voting Assistance Program on behalf of the Secretary of Defense.

The UOCAVA absentee registration and voting process includes steps to be completed by voters and local election officials. (See Section 3 for a description.)

DoD decided to initiate this new demonstration project by building on the technical foundation begun with the 2000 Voting Over the Internet (VOI) pilot project, again using a remote Internet registration and voting system. Security is an important issue for any voting technology, and a great deal of engineering expertise was applied to the task of designing and developing a robust and highly secure registration and voting process.

Two external technical groups were convened to provide independent peer review of the security engineering work. The Federal Information Assurance Group (FIAG) was composed of technical experts from several federal agencies with responsibility for the nation's critical information infrastructure: the Office of the Secretary of Defense, the National Security Agency, the Central Intelligence Agency, and the National Institute of Standards and Technology. This group reviewed the Internet registration and voting threat risk analysis prepared for the project and commented on the threats identified, the probability of their occurrence, the degree of harm that might result, the possibility of detecting various types of attacks, and what preventive and/or mitigating strategies could be employed.

The second group was called the Security Peer Review Group (SPRG) and was composed of ten experts on computer security and voting systems drawn from academia and the private sector. The participants selected represented a range of views regarding the security and reliability of electronic voting, and the use of the Internet for voting. Since the project results were to be reported to Congress with recommendations for future demonstrations, FVAP thought it appropriate to involve a variety of viewpoints to provide a balanced assessment of this technology for consideration by the policymakers.

After two meetings, four members of the SPRG posted a critique of the computer and communication security issues of the SERVE voting system on a website and issuing a press release calling for the project’s termination. Observing that this situation could undermine public confidence in the system, Deputy Secretary of Defense Wolfowitz decided on January 30 that the system would not be used for the 2004 election. Shortly thereafter, all work in progress to complete the system documentation, conduct independent testing for system accreditation, and prepare for system deployment and training was terminated.

While not taken to its intended conclusion, the project nevertheless yielded a considerable amount of useful information and lessons learned for the design and certification of electronic registration and voting systems, and for the conduct of future demonstration projects. This report does not emphasize the specific technology solution developed since the certification was not completed and the system was not deployed and used. Instead, it focuses on the project methodology and analytical results, as a contribution to the on-going national dialogue on election administration issues and voting system technology concerns.

1.2 Report Overview

This report has eight sections and four appendices. Section 2 provides the legislative background and description of the SERVE project, its objectives and scope, and the roles and responsibilities of the participants. Section 3 outlines the barriers faced by UOCAVA voters and how the SERVE solution would have addressed these barriers. Section 4 presents a statement of design principles for a remote Internet registration and voting system and details how these principles were applied in the SERVE system. Section 5 discusses the issue of accrediting a voting system when it employs technology not covered by existing standards and how this issue was resolved. Section 6 overviews the evaluation design that was to have been used to evaluate SERVE. Section 7 identifies the major implementation issues that SERVE encountered and how they were addressed. Section 8 concludes with lessons learned and moves nine recommendations to consider for future demonstration projects.

The four appendices of this report provide technical details of various elements of the SERVE project that will be of interest to specialized audiences. The first appendix provides a description of the SERVE system and a functional overview. The second appendix is a detailed presentation of the SERVE security architecture, while the third appendix discusses system requirements. The fourth appendix gives the project's deployment strategy. These appendices are available electronically at http://serveusa.caltech.edu.

2. DESCRIPTION OF SERVE

2.1 Legislative Authorization

Section 1604 of the Fiscal Year 2002 National Defense Authorization Act (Public Law 107-107) directed the Secretary of Defense to carry out a demonstration project enabling absent uniformed services voters to cast ballots through an electronic voting system in the 2002 general election. The project was to be carried out through cooperative agreements with state and local election offices. The results of the demonstration were to be reported to Congress along with appropriate recommendations on whether to continue the project on an expanded basis for future elections. The Director, Federal Voting Assistance Program (FVAP), who administers the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) on behalf of the Secretary of Defense, was responsible for this project. The project title, Secure Electronic Registration and Voting Experiment (SERVE), was derived from the statutory language.

The legislation made provision for delaying implementation of this project until the November 2004 general election, with appropriate notice to the relevant Congressional committees. As described in Section 1, since the authorizing legislation was not signed until late December 2001, there was not sufficient time to define and field a project for the 2002 election. So a notification letter was sent from the Secretary of Defense to the Senate and House Armed Services Committees in May 2002 requesting approval for a 2004 implementation.

In October 2002 staff members of several Congressional committees were briefed on the SERVE concept, scope and evaluation approach, which included overseas citizens. Many overseas citizens, such as DoD employees and support contractors, face the same barriers to voting as military personnel. In addition, a key element of the evaluation was to examine impacts for a variety of voter scenarios, so the inclusion of overseas non-military citizens enriched the analysis base.

2.2 Project Objectives

The principal objective of SERVE was to assess if the use of electronic voting technology could improve the voting participation success rate for UOCAVA voters. This entailed defining and conducting a demonstration effort whereby a sufficient number of voters could cast ballots in the general election to produce statistically meaningful data. Impact on voter participation success would be evaluated based on several subcategories of UOCAVA voters: e.g., active duty military based in the U.S., based overseas, and forward deployed; activated Guard and Reserve units; military dependents; federal employees overseas; private sector overseas citizens.

A second objective was to assess the potential impact on state and local election administration of an automated alternative to conventional by-mail absentee registration and voting. It was determined that a cross-section of election jurisdictions should be recruited in order to present as representative a picture as possible, given the variability of election administration processes and procedures across the country.

Thus, the project was structured to address these research questions:

1. Is remote Internet registration and voting an effective, affordable and secure method to improve absentee Uniformed Services and overseas citizens' access to the polls?

2. What do we need to know to implement this type of system as an alternative to the traditional by-mail process?

2.3 Project Scope

2.3.1 Recruiting Participants: States and Counties.

Achievement of the SERVE research objectives was dependent on the number of volunteer voters and which states and local jurisdictions decided to participate. The first recruiting effort was aimed at the states. A planning meeting was held in November 2001 with several state and county election officials and representatives of NASS, NASED and IACREOT to get their input and assistance in fleshing out the preliminary project concept. At that time the passage of the enabling legislation appeared to be imminent. The timeline called for sending letters of invitation to the 55 UOCAVA jurisdictions by the end of November with the expectation of finalizing the list of participating states by the end of January 2002. Since the legislation did not become effective until the end of December, the first round of state invitation letters was sent in January 2002 with a request to commit to state participation by March 2002.

The timeline for commitment slipped due to a variety of factors: some states needed to pass enabling legislation, many had staffing and budgetary constraints and were concerned about additional workload, turnover in state and county election personnel affected ability and/or interest level in participating, Help America Vote Act (HAVA) state plan preparation workloads occupied critical resources and staff, several states were preparing or conducting voting system procurements, other state and county election administration initiatives needed to be given priority. Additionally, several states were transitioning to statewide voter registration systems, some jurisdictions had small UOCAVA populations, and some jurisdictions were not prepared to work with the level of automation that SERVE entailed. The final cutoff for participation was announced in July 2003, more than a year after originally scheduled.

The following list reflects jurisdictions participating in SERVE as of January 20, 2004, with asterisks identifying counties with pending participation as of that date.

Arkansas: Benton County, Boone County, Craighead County, Crawford County, Faulkner County, Jefferson County, Pulaski County, Washington County

Florida: Bay County, Clay County, Miami-Dade County, Okaloosa County, Orange County, Osceola County

Hawaii: Hawaii County, Honolulu City and County, Kauai County, Maui County

North Carolina: Craven County, Cumberland County, Onslow County, Pasquotank County, Wayne County

South Carolina: Aiken County, Anderson County, Beaufort County, Calhoun County, Colleton County, Florence County, Greenville County, Lexington County, Orangeburg County, Pickens County, Richland County, Spartanburg County, Sumter County, Williamsburg County, York County
Lancaster County*, Greenwood County*, Chester County*, Cherokee County*, Marlboro County*

Utah: Davis County, Sanpete County, Tooele County, Utah County, Weber County

Washington: Cowlitz County, Island County, Kitsap County, Pierce County, Spokane County, Snohomish County, Thurston County

2.3.2 Recruiting Participants: Voters.

A target of 100,000 voters was set to provide the necessary population base for meaningful analysis. This number is approximately 1.5% of the estimated 6,000,000 UOCAVA eligible voters worldwide; the UOCAVA population is about 3% of the total national population eligible to vote. These are rough estimates, as there is very little consistent or reliable data at the state or county level to identify potential UOCAVA voters. Some election jurisdictions record information on “military voters”, but these data are often incomplete and not well maintained. Until the Help America Vote Act was passed there was no federal requirement for local election officials to keep information on UOCAVA voters. The only available national estimates of the potential UOCAVA-eligible voter pool were higher than what local election officials were able to identify as UOCAVA voting activity.

The voter recruiting effort began in June 2003 when the SERVE public website, SERVEUSA.gov, went live. The website published information about the project, listed the participating jurisdictions, and provided an e-mail link for interested voters to sign up to be notified when the system became available for use. There were approximately 400 interested voters on the notification list at the time the project was terminated. A more focused voter outreach effort was poised to get underway in early 2004.

2.3.3 The System Acquisition Strategy.

FVAP decided to build on the foundation of the 2000 Voting Over the Internet (VOI) pilot and again use a remote Internet registration and voting system as the vehicle for the demonstration. This type of system envisioned allowing the voter to register and vote using any computer with Internet access anytime, anywhere. It also would allow the voter to register from one physical location and vote from another without having to notify his/her election official of an address change. This flexibility of access and location independence is especially well suited to the circumstances of UOCAVA voters.

In July 2001 FVAP began a market survey of voting system vendors to assess the state of the art of existing registration and voting technology. The purpose was to determine if there were any commercial products or systems available that could be used as is or modified for SERVE. While a wide variety of systems from nearly every U.S. vendor were examined, no comprehensive solution was found. No system had voter registration as an integrated component and none provided a sufficient level of voter authentication or security for a remote registration and ballot transmission system. In addition, most of the systems were not designed to operate over the Internet. However, there were several existing products that had potential for being modified to meet the SERVE requirements. So the decision was made to structure the procurement strategy for the system development effort to favor the adaptation and integration of existing products instead of building an entirely new system. This was expected to reduce project risk, time and cost.

2.3.4 Description of the SERVE System.

The SERVE system was designed to provide all the functions of a complete election administration system for UOCAVA voting. Local election officials would use it as an adjunct to their existing local systems. These local systems, such as voter registration, would continue to be the system of record. The SERVE system included the following capabilities for election officials: identification and authentication, enrollment, system setup; voter registration and absentee ballot request application processing; election definition, ballot conversion and proofing; voted ballot receipt and reconciliation; ballot tabulation; and reporting.

The following capabilities were provided for voters: identification and authentication enrollment[2], voter registration and absentee ballot request application submission, status checking, absentee ballot availability notification, absentee ballot delivery and voting, ballot choice confirmation, and voted ballot return. See Appendices 1 and 4 for further description of the system's capabilities.

The system developed for the SERVE project was called the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Voting System (UVS). As illustrated in figure 2.1, the UVS system architecture consisted of a central server environment that hosted all the voter functions, all data, and all the election administration functions except ballot tabulation. A dedicated laptop would be provided to each participating jurisdiction for the function of downloading the anonymous voted ballots, decrypting the ballot data, and tabulating the results. To use UVS, an authorized local election official (LEO) could log on to the central host from nearly any Windows-compatible computer in their office, authenticate themselves using a digital signature through the Identification and Authentication (I&A) Subsystem, and access any function for which they were an authorized user. Similarly, any voter who had been issued a SERVE digital signature could access any of the voter functions from any Windows-compatible computer. No special software was required to be installed on any LEO or voter computer. UVS systems operations staff performed standard system administration functions. All operations staff were required to have a digital signature on a smart card to access the UVS Central Hosting Environment. Appendices 1 and 2 provide more detailed information.

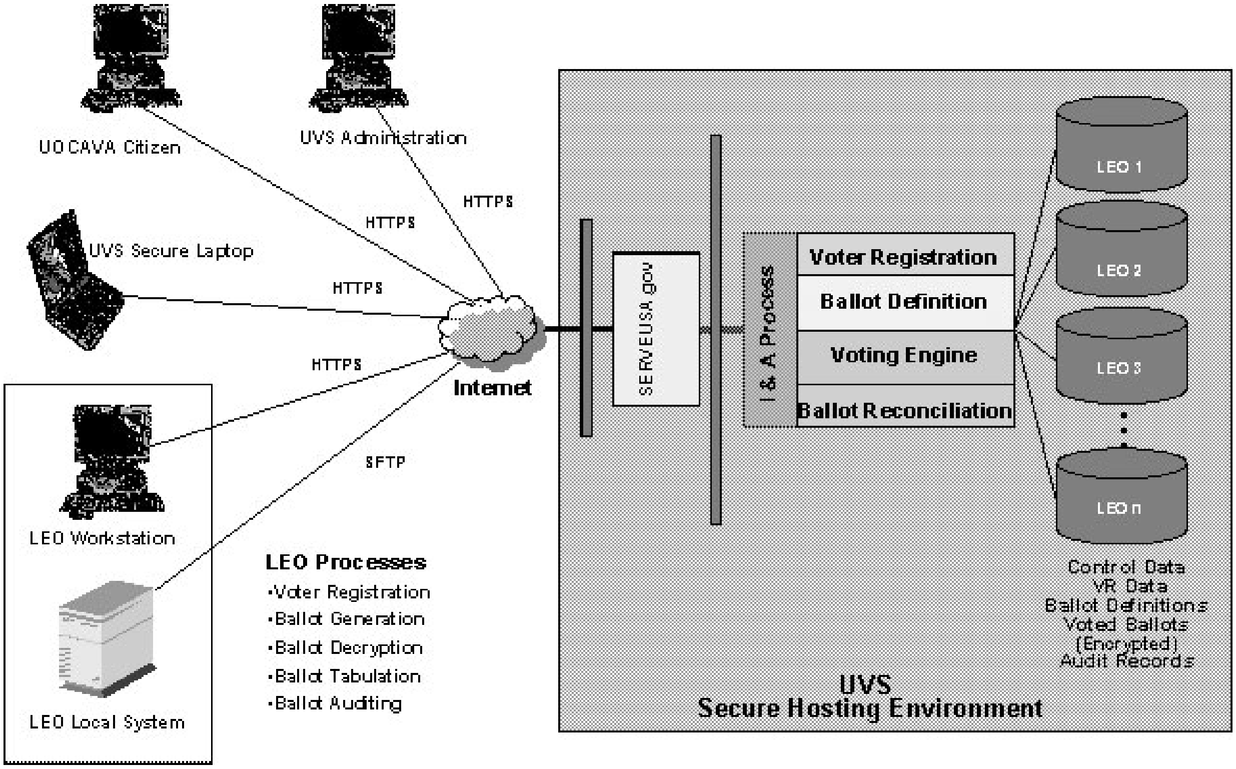

Figure 2.1 UVS Central Hosting Environment

2.3.5 The System Implementation Approach.

The Voting Over the Internet findings made it clear that any future project needed to be more integrated with local election office processes and systems to provide a realistic demonstration environment. Consequently, the initial SERVE implementation approach was to develop electronic interfaces between the SERVE system and local election administration systems. This was viewed as a way to minimize additional workload for LEOs by eliminating the need for them to manually pass data between local systems and the SERVE system. However, this turned out not to be feasible in many cases for a variety of reasons. (See Section 6 and Appendix 4 for further discussion.) The end result was that about 60 percent of the counties were planning to use the SERVE system in parallel with their existing systems.

2.3.6 Developing System Requirements.

The Voting Over the Internet (VOI) pilot project in 2000 provided voter registration, ballot conversion, voting and ballot delivery capabilities, which was a good starting point, but the SERVE system needed to provide a complete election administration solution. The initial concept was to define a basic system that would incorporate all the business rules required by all the participating states, with variations in values, such as filing deadlines, being handled by parameters that could be set individually by each local jurisdiction. A significant lesson learned during SERVE development was that there are logically conflicting business rules in various state election administration processes that could not be readily accommodated with a standard software application. This resulted in the development of manual workaround procedures for some jurisdictions.

A great deal of effort was put into assembling a comprehensive set of requirements for the SERVE system. This work was carried out in multiple waves. First the VOI requirements were analyzed for applicability. The election codes of states that had expressed an interest were reviewed to gain familiarity with the statutory requirements of potential participants. Then a series of site visits was conducted with state and county election personnel to document their work processes and administrative procedures and to get an understanding of how statutory provisions were interpreted. In addition, detailed technical information was collected on local systems as a basis to begin defining data exchange interfaces.

A Preliminary Design Review was conducted in January 2003 and the notional system functions and processes were briefed to representatives of 15 states and 14 counties with an interest in participating. Their feedback was used to refine the design concepts so that development work could begin. This meeting was followed by a Critical Design Review in March 2003, where revised and refined functions and processes were presented. A major concern—even at this late point—not all of the states and LEOs were completely committed to participating in SERVE, nor did many participating jurisdictions completely understand the functionality of the system. This meant that new requirements could surface after the design needed to be frozen. Finally, a hands-on “test drive” was held in December 2003, once the system development was nearly complete. The test drive provided an opportunity for local election officials to use the software and determine how well it would serve their needs.

While these high level reviews provided useful input to the system design effort, there were many detailed design alternatives, issues of appropriate wording and on-screen presentation, and other questions that arose in the course of development that needed quicker resolution. So a Design Advisory Group (DAG) was established to provide quick turnaround review and to answer questions from the system developers. This group was comprised of one or two representatives from each of the participating states. It was their responsibility to get consensus from the counties and/or agreement from their state election officials on how best to handle these questions. This group was chaired by a former election official who provided invaluable assistance in translating some of the more technically worded questions into language more readily understood by the DAG members. This person also helped to interpret their responses back to the development team. This subject matter expert also spent considerable time reviewing various elements of the system as they were being developed, helping the software engineers understand the nuances of election administration, and reviewing documentation. This turned out to be a very effective methodology that contributed to the practical utility of the system design as well as an efficient way to keep users who were widely distributed around the country meaningfully engaged in the process.

2.3.7 Defining System Accreditation and Certification Methodology.

The accreditation and certification process for SERVE was more complex than for most voting systems. There were several reasons for this:

- SERVE was designed as a consolidated system performing voter registration, election administration, voting, vote tabulation, and other functions. While it was clear that the 2002 Voting System Standards (VSS) should be applied to the voting and vote tabulation functions, there are no prescribed standards nor any accreditation process for voter registration and many of the other system functions.

- SERVE was a web-enabled, Internet-based system with different operating modes and access methods than software-based voting systems that are used at polling places. It contained technology components and features that were not covered by the current VSS. Therefore, there were no prescribed standards or accreditation process for these components; nor any significant precedent in interpreting the VSS for these circumstances.

Federal government computer systems that process sensitive information are required to go through a system certification process. In a sense, SERVE was a federal government system because its development was being funded by the Department of Defense (DoD). However, no one from DoD had system access; only state and local election officials were authorized to use the system and its data. In addition, all the data stored and processed by the system was “owned” by the state and county election offices; there was no DoD information on the system. However, DoD does have well-defined processes and standards for secure computer system certification. The SERVE system could be characterized using the same criteria and methodology, so FVAP elected to model the SERVE certification process on these well-established DoD practices.

2.4 Federal, State and Local Roles and Responsibilities

SERVE was a cooperative federal, state, and local government undertaking. Pursuant to the mandate in the FY02 Defense Authorization Act, the Director, Federal Voting Assistance Program was responsible for overall funding, project planning, and project management. FVAP and each of the participating states signed a Memorandum of Understanding that defined the roles and responsibilities for FVAP, the State election office, and the participating county election offices. In some states, the election process was handled at the state level and at some it was handled at the county level. The following is a listing of the roles and responsibilities for FVAP and the States/Counties.

2.4.1 **Federal Voting Assistance Program**

(a) Provide oversight and management of the SERVE program.
(b) Secure and provide funding for system development, implementation, and deployment; system certification; and SERVE program evaluation.

(c) Provide central system hosting, applications software, and documentation for the UOCAVA Voting System (UVS) with flexible implementation alternatives for State and county participation.
(d) Provide a laptop and software for ballot decryption and tabulation (UVS laptop) at each State or county location where tabulation will occur.
(e) Provide training for use of the system.
(f) Provide digital signatures for all designated State and local election office personnel and local computers, as required.
(g) Specify policies, procedures, and standards for UVS implementation and operation.
(h) Provide Help Desk support during the period of UVS operation in 2004.
(i) Provide public affairs information and guidance.
(j) Coordinate SERVE program activities and policy issues with participating States and counties and other organizations, as required.

2.4.2 State/County

(a) Assist the SERVE Team in development of system technical and functional requirements.
(b) Assist in development of SERVE policies, procedures and standards.
(c) Provide timely feedback on system requirements, security policy, certification standards, evaluation reports and other project documents, as required.
(d) Designate a single representative to the UVS Design Advisory Group.
(e) Assist in recruiting potential voters to participate.
(f) Provide an Internet account.
(g) Sign software license agreement.
(h) Choose an implementation alternative for participation.
(i) Designate personnel who will be authorized to use the UVS.
(j) Participate in system training.
(k) Participate in certification process, as required.
(l) Collect and report evaluation data.
(m) Return all equipment supplied by SERVE at the conclusion of the program.

Several states required enabling legislation to participate in SERVE. These states did not have existing legislation to allow for Internet-based voting. This was a lengthy process involving state election personnel, state legislative committees and testimony provided by the Director, FVAP to the state legislatures.

Active participation by State and county officials was essential for the success of the project. These officials were the source of the requirements for the SERVE system. They spent many days describing and walking through their particular election administration processes in detail. They helped the design team understand, translate and apply current business processes for the implementation of an election administration system employing new technology and based on a radically different operations and management model. They worked with the development and implementation teams to assess how best to integrate the SERVE system with their local election administration systems and to develop and in some instances test, the technical and/or procedural interfaces most appropriate to each county's situation. County participation involved election staff, IT support staff and often state vendors for Voter Registration, election admin, voting and tabulation systems.

State and County officials participated in FVAP site visits at the state or county and project meetings held in the DC metro area. Travel expenses for the alternate meetings were reimbursed by the project and then by the States/Counties. All staff time was donated by the participating jurisdictions. In many instances, voting system vendor time was also contributed.

2.5 Timeline

The original timeline was as follows.

2002	
Sept. 27	State Commitment to Participate
Mid-October	Brief Congressional Staffers
Nov. 29	Establish Executive Steering Group
Dec. 31	Complete Requirements Validation
2003	
Jan. 22/23	Conduct Preliminary Design Review
Feb. 19/20	Conduct Critical Design Review
May 2	Complete Specification of Certification Requirements
Sept. 1-Mid- Sept.	Begin Deployment/Training to Test LEOs
	Activate Help Desk
Oct. 1	Begin ITA Certification Testing
Nov. 14	Complete Certification Testing
Dec. 31	Complete Deployment/Training to all LEOs
2004	
Jan. 1	SERVE System Available for Registration
Feb. to Sept.	Primary Voting
Mid-Sept. to Nov. 3	General Election Voting
December	Close SERVE System
2005	
March	Complete Draft Report to Congress
June	Deliver Final Report to Congress

During the last quarter of fiscal year 2003 schedule changes occurred in the system development effort and project execution due to: delays in state commitments (extending the requirements analysis period); extended software development period (requirements for the central system were more complex than estimated); having two releases of the system software versus one (necessitating additional accreditation testing) and local system integration was more complex than originally estimated.

The final schedule was as follows.

2003	
January – December	Develop System
2004	
January	Begin citizen enrollment
	Begin ITA Certification Testing
March	Complete ITA Certification Testing
March/April	Voter registration
April – June	Deploy county laptops
July – November	Primary and general elections
2005	
March	Complete Draft Report to Congress
June	Deliver Final Report to Congress

3. Barriers to Voting and How SERVE Addressed Them

3.1: Barriers to Voting for the UOCAVA Population

After each presidential election, the Federal Voting Assistance Program conducts a survey of Local Election Officials (LEOs), Voting Assistance Officers, and UOCAVA voters to collect information about each group's experience in the election. Based on the survey results for the 2000 election, the FVAP identified an array of problems that LEOs experience in processing Federal Post Card Applications (FPCAs). The FPCA is the form used by UOCACA voters to register to vote and to request an absentee ballot.

- 73% of LEOs responding reported at least one incidence of no or inadequate voting residence address information
- 35% of LEOs responding reported at least one incidence of inadequate or illegible mailing address information
- 26% of LEOs responding reported at least one incidence of applicants applying to the wrong jurisdiction
- 23% of LEOs responding reported at least one incidence of illegible writing
- 18% of LEOs responding reported at least one incidence of no signature
- 18% of LEOs responding reported at least one incidence of the FPCA received too late

FVAP also reported data on responses received when voters were asked the reason why they did not vote. These responses are broken down by a voter's status under UOCAVA—uniformed services, federal civilians, or non-federally employed overseas civilians. The most common problem identified in the post 2000 election survey was that voters did not know how to get an absentee ballot. The next most common problems were that voters do not receive an absentee ballot at all, they received the ballot too late, or the process of absentee voting discouraged them.

Of the Uniformed Service members who did not vote in the 2000 election, 22% responded that they had not received a ballot and seven percent reported receiving their ballot too late to return it by the state's deadline.

Data from numerous studies and analyses conducted since the 2000 election show that civilians living overseas and personnel in the uniformed services have difficulty participating in the electoral process using the current by-mail absentee voting system. In separate reports, the United States General Accounting Office and the Department of Defense Inspector General found that perceived confusion of the UOCAVA voting process resulted in many voters being disenfranchised.[3] The problems include:

- Procedures for UOCAVA voting vary by state. For example, the deadline for registering as a UOCAVA voter ranges from 30 days prior to an election in 21 states to no registration requirement in 15 states. Similarly, ballots in some states have to be received prior to Election Day in 4 states, but can be received after Election Day in 15 states. This causes confusion for voters when they discuss absentee voting with their associates who may be from different states.

- Military UOCAVA voters and civilians in remote geographic areas suffer especially from problems in voting because of physical logistical difficulties.
- The paper-based process is also a source of many problems. As the GAO noted,

  > "[M]ilitary and overseas voters do not always complete absentee voting requirements or use federal forms correctly. The basic steps that absentee voters must take to register and request an absentee ballot are similar for all states. Nevertheless, absentee voting schedules and requirements vary from state to state…. County officials said that problems in processing absentee voting applications arise primarily because voters do not fill in the forms correctly or do not begin the voting process early enough to complete the multiple steps they must take."[5]

- Ballot transit times are another important potential problem. In their study of UOCAVA voting during the 2000 election, the GAO found that transit times for first class mail can range from as little as five days to as much as a month.
- A survey by the GAO found that almost two-thirds of all disqualified absentee ballots were rejected because election officials received them after the official deadline. For UOCAVA voters, approximately 10 percent of the ballots were rejected because the envelope or the form accompanying the ballot was not completed properly. For example, many absentee envelopes lack the required signature or valid residence information.[6]
- The DoD Inspector General also noted that there are special types of mail transit, such as transit to naval vessels underway that can be difficult to service. For example, mail transit averages 7 days for 80 percent of mail. However, remote areas and forward deployed locations, such as Bosnia or Kosovo, may take an average of 9 days.[4]

3.2 The By-Mail UOCAVA Voting Process

The survey data and other analyses illustrate the problems associated with the traditional by-mail UOCAVA absentee voting process. In the voter registration and absentee voting process there are five basic steps. First, a citizen must register to vote. Second, the voter requests an absentee ballot. These two steps may be completed simultaneously by using the Federal Post Card Application. Third, the local election official sends the absentee ballot to the voter. Fourth, the voter completes and returns the absentee ballot. Fifth, local election officials verify the identity of the voter and determine if the absentee ballot meets state and legal requirements in order to decide whether or not to tabulate the absentee ballot. The main difference between traditional absentee voting and UOCAVA absentee voting is the fact that the citizen is not located in their voting jurisdiction, either to request the ballot or to receive the ballot which can cause delays in the process.

The UOCAVA citizen obtains the "Federal Post Card Application" (FPCA) from a Voting Assistance Officer (VAO), FVAP (via website, email or telephone) or LEO. The FPCA is a standard federal form acceptable in all states and territories. The FPCA allows UOCAVA citizens to both register and request an absentee ballot in a single step. The citizen completes the form manually, following any specific procedures for the state or locality in which they are registering and requesting an absentee ballot. They affirm the request by signing and dating it (and for some states a witness is also required). The citizen then sends the FPCA form to the LEO. Many states allow the FPCA to be transmitted by fax. State law usually requires that the original form be mailed so an original "wet" signature is received.

The key problem that might occur in this stage is that, given the lack of national uniformity in voter registration requirements—especially deadlines for registering prior to an election—a voter may not follow the specific registration rules for their state. Problems can also arise if required areas of the form were not completed, no voting address or an inadequate address were provided, an inadequate or illegible mailing address was provided, the handwriting was illegible, the form was not signed, a date of birth was not provided, or the individual failed to provide a partisan preference for primary elections. Any of these problems with the FPCA can lead to a UOCAVA citizen being disenfranchised. As the GAO noted, "[M]ilitary and overseas voters do not always complete absentee voting requirements or use federal forms correctly. …County officials said that problems in processing absentee voting applications arise primarily because voters do not fill in the forms correctly or do not begin the voting process early enough to complete the multiple steps they must take."

During the second stage in the process the LEO receives the request, processes it, and sends an absentee ballot to the voter when it becomes available. Here, transit time becomes an important potential problem. The GAO has found that transit times for first class mail can range from as little as five days to as much as a month. Transit time in the UOCAVA absentee ballot process is complicated because it is often the case that two documents—the voter registration/ballot request form, and the ballot—must travel back and forth between the LEO and the voter. Thus, the transit time for a given document must be doubled under the existing by-mail process; if an absentee ballot can be delivered to a voter in a week, it will take at least two weeks in total transit time for the ballot to be cast successfully.

In the third stage of the process, the voter receives the absentee ballot in the mail and completes the ballot manually. The voter must make sure to follow any specific state requirements for absentee voting (which are included in the ballot package), and must sign and date the ballot-mailing envelope. The voter then returns the ballot to the LEO through the mail, where the postmark (or dated signature) dates the ballot. If an overseas military or civilian voter does not receive an absentee ballot in the mail from the LEO, they can obtain, vote and submit a "Federal Write-In Absentee Ballot" (FWAB) for federal races.

3.3 Overcoming UOCAVA Voting Problems with Technology

The 2000 FVAP post-election survey identified a range of problems that existing technology—especially Internet registration and voting—can potentially alleviate or resolve. The "Voting Over the Internet" (VOI) pilot project conducted in 2000 demonstrated how technology could address these problems; SERVE would have tested the broader application of the VOI findings. The VOI proof-of-concept determined that:

1. Internet voting could eliminate the problems of illegibility and incompleteness of FPCAs. The electronic version of the form does not allow the voter to submit the form until all required fields are completed.
2. The ballot transmission problems are resolved, since a voter can access their ballot instantly once it becomes available and, when cast, is received by the LEO instantly.

3. As with the FPCAs, the electronic voting eliminates incompleteness of ballots by requiring voters to complete all aspects of the absentee ballot—such as "signing" the ballot—before it is submitted.
4. Enabled voters to determine their registration state, when ballots were available and to confirm that the ballot was received by the LEO.
5. Eliminated the problems associated with voters changing physical addresses between the time of registration and the time of the election.

In short, SERVE would have addressed the key problems that were identified in the FVAP post-election survey and in the analyses conducted by the GAO and DoD Inspector General. It was designed to have enabled UOCAVA voters to register more effectively by eliminating form omissions, allowed these voters to receive their ballot instantaneously, and to return their cast ballot instantaneously. It would have allowed voters to check their status independently. Electronic registration and voting technologies are generally recognized to allow a voter to cast a more accurate ballot compared to paper systems, since they allow a voter to review their vote choices before final submission and to use the technology to help correct common voting errors (like over- and undervoting).

3.4 The Internet Advantage Over Other Electronic Voting Methods

Internet voting, in theory, reduces traditional mail ballot transit time to almost nothing. Internet voting as designed using the SERVE system preserved the secrecy of the ballot and utilized a secure mechanism to ensure the ballot was received by the LEO and then counted.

How the voting needs of the UOCAVA population can be served by technological improvements can be conceptualized on three dimensions. The first dimension is ballot transit time, which has three components: the voter's registration and absentee ballot request; the sending of a ballot to the voter by the LEO; and the return of the completed ballot from the voter to the LEO. The second dimension is the privacy of election materials when they are being transmitted between voter and LEO. The third dimension is the relative accuracy of different technological means of correctly capturing a voter's intent (in particular where the absentee voting mechanism allows voters to check their ballot for errors).

Relative to the traditional, by-mail, absentee registration and voting process that now exists for UOCAVA voters, there are a number of alternative electronic technologies that have—or could— be used to mitigate problems on each of these dimensions.

1. Fax technologies have been used to get ballot materials to voters, and by voters to return their ballots.
2. Email has been used to get ballot materials to voters.
3. Downloadable ballot materials have been provided to voters via the World Wide Web.
4. Dynamic ballot materials have been built by LEOs on their websites that voters could use to produce a printable ballot on their local system that could then be returned to the LEO.
5. Internet registration and voting systems have been used to allow UOCAVA voters to exercise their franchise.

4: Design Principles for an Internet Registration and Voting System

The SERVE system was designed to parallel the existing vote-by-mail, UOCAVA absentee voting process described in Section 3.

Through the SERVE development process, a series of design criteria were developed regarding the features that an Internet voting system should include. These criteria reflect the input of various participants in the development and review of the system and reflect general design principles that should be the focus of the development of Internet voting systems in the future. We have divided these criteria into four categories: (1) security, (2) usability, (3) process, and (4) auditability.

4.1 Security

Security is the paramount issue that must be addressed in the conception, design, creation and operation of a voting system. A voting system must be designed with these same features; providing a highly secure, robust and reliable system that gives the electorate confidence that their vote will be counted as intended.

To provide this high degree of security, the SERVE security design assumed that no single part of the system could, individually, be trusted fully. Instead, the design relied upon multiple layers of redundant checks and balances (defense-in-depth) throughout the hardware, software and human elements of the system. THE SERVE system was designed with mechanisms to check the veracity of any transaction, both within the system and with external systems, such as the Internet and a voter's personal computer. This was done so that the system could both protect itself from the other systems and check for the correct operation of the other systems.

One critical facet of the SERVE project was that it conducted an analysis of the threats that exist in both the by-mail and Internet voting procedures. Without this analysis, it is difficult to critique SERVE because there is no baseline on which to base the critique. For example, a denial of service attack can happen in both the paper-based UOCAVA absentee voting process and with Internet voting. Although the two threats manifest themselves differently, they have the same effect of disrupting the conduct of an election. By comparing the threats and their likelihoods across voting platforms, policy makers are better equipped to determine which threats are more or less viable. This analysis needs to be continually updated as the threats and risks associated with various forms of voting change, and as new technologies are proposed for registration and voting.

Table 4.1: Threat Comparison Between By-Mail System and SERVE

Threat	**Skill Needed**	**Consequences**	**Realistic**	**Countermeasures**	**How it happens in the paper by-mail system**	**Comments**	**How SERVE mitigated threat**
Denial of service attack	Low	Voter disenfranchisement; possibly selective disenfranchisement	Already occurs, whether by intent or not, in the current system	No simple tools; requires many optional means of delivering paper ballots and would require a method that bypasses foreign postal services; attack can be launched from many different places	Vagaries of US and foreign mail service can delay ballots delivery or return.. Rapid deployment forces are often not stationary long enough to get a ballot delivered to where they are (as opposed to where they were anticipated to be when they requested). Foreign mail carriers outside the scope of US law could hold up absentee ballots so they are received late or destroy them. They could also intercept them on their way back from the voter, so the voter may well never know. This could also be done by insiders in the USPS or in the military mail program. A simple failure to postmark envelopes is enough to disqualify the ballots in many states; this could be done on a selectively or universally..	Best information today indicates that this is not a hypothetical risk in the current system, but a reality. 20 – 29% of voters surveyed say they do not get their ballot at all or don't get it in time to cast. A GAO report of small counties showed that 8% of ballots received were rejected for various reasons. Only method to counteract would be to somehow provide a replacement ballot to the voter. Not possible in time to allow the vote with the paper by-mail system. FAXed ballots have been used to alleviate these risks, but the voter loses ballot secrecy	Eliminated mail transit time and involvement of foreign postal services. Automatically time and date stamped all ballots, eliminating postmark problems. Encrypted transmissions to prevent tampering en route. Signed ballot to detect tampering en route.
Specific attack on a single ballot to prevent voting	Low	Voter Disenfranchisement	Many possible ways to keep a ballot from being received or returned by the voter,, or received by the LEO	Request new ballot	Individual absentee ballots can be stolen or delayed en route to the voter or stolen once they have been received by voter. Also, see Denial of Service above.	There have been documented cases of organized efforts to intercept absentee ballots. Given the time constraints, voters have few recourses in the current system if their ballot is intercepted.	Encrypted ballot retrieved directly by the authenticated voter upon request to prevent tampering enroute. If problems occur receiving the ballot, voter can go to another PC and request the ballot again.
Electioneering	Low	Voter annoyance, frustration, distraction, improper influence	Occurs today	Voter can find a secluded place to complete their absentee ballot	Because no election officials preside over absentee balloting, electioneering could take place at any location where absentee paper ballots are received or voted.		None. In absentee voting, the voter has control of the information they review while casting their ballot.

Threat	Skill Needed	Consequences	Realistic	Countermeasures	How it happens in the paper by-mail system	Comments	How SERVE mitigated threat
“Spoofing” of Absentee Ballot	Low	Vote theft, privacy compromise, disenfranchised voters	Relatively easy to carry out	None exist; likely to go undetected	Hackers could obtain list of voters who register absentee (or list could be obtained by insiders). This is public information in many states. Fake absentee ballots could be developed and distributed by attackers to large groups of these voters. These ballots could have incorrect addresses for returning to LEO, or unacceptable formats, thus keeping them from being counted.		SERVE provided voter with ability to confirm if their ballot was received. If large numbers of ballots were somehow spoofed, it is likely that some voters would have alerted LEOs and countermeasures could be launched. SERVE also provided LEOs with a means of reporting which ballots were counted and the reasons why some ballots were rejected.
Insider attack on system	Low	Compromise of election	Insider attacks are the most common, dangerous and difficult to detect of all security violations	Many tasks in election systems require action by two or more people, requiring collusion of insiders for successful tasks. Some tasks occur with public observers.	Insiders can deliberately destroy received absentee ballots and claim they were not received; likely undetected. Insiders could also modify the software used to tabulate paper absentee ballots could do so in a way to modify only enough votes to impact the election.	Modification of ballot tabulation software code has occurred.	SERVE provided no means to destroy ballots, only to reject them. Audit trails in SERVE processing maintained an audit trail of all significant events. Software that produced audit trails is hash-controlled so that any modification of that software can be immediately detected. All tabulation actions could be repeated, including reversal of ballot rejections if warranted, on different tabulation equipment using records maintained on the central server so long as the LEOs private key is available.

Threat	Skill Needed	Consequences	Realistic	Countermeasures	How it happens in the paper by-mail system	Comments	How SERVE mitigated threat
Vote buying and selling	Medium	Violation of one-person, one-vote principle of elections	Vote buying schemes have a long history in American politics	Criminal penalties are a disincentive in jurisdictions where they apply (penalties may be difficult to apply to attacks from some countries)	Attackers from any location could solicit voters to send paper ballots to a special address, filled out and signed (but not sealed), with only the race to be impacted left blank. The Internet provides new means to advertise these offers (note the Nader/Gore vote swapping sites in 2000). Attacker then fills in the ballot for the race to be impacted, seals the ballot and sends it in, then sends payment to voter (or not). Twist on this is to solicit votes, have ballots sent to a PO box that is not checked or traceable or address that is abandoned property, and then not send the ballots in at all, effectively depriving the voter of any vote and decreasing the attacker's risk of capture. A third alternative is for voters to send copies of their completed absentee ballots (via fax, mail or email) to the vote buyer.	Level of trust voter must have that a) their ballot will be passed on and eventually counted, and b) they will receive payment. The second of these is also a trust issue with any vote buying/selling scheme. As with any such scheme on any kind of voting system, the advertising to reach a large enough pool for a cooperative attack to be successful would increase the likelihood of detection. Physical address required if the ballot is to be sent on would also increase likelihood of capture. Voter could contact LEO to have purchased ballot invalidated, but given potential ballot transit time delays this is infeasible for many UOCAVA voters.	Voter could not use SERVE to produce a final receipt that indicates how they vote. Voter's could still change their choices while their choices are visible and printable. The ability to change requires a vote buyer to trust the voter's word that a printout matches their vote. Voter could also contact LEO to have purchased ballot spoiled and new ballot issued.

Threat	Skill Needed	Consequences	Realistic	Countermeasures	How it happens in the paper by-mail system	Comments	How SERVE mitigated threat
Coercion	Medium	Voter disenfranchisement; violation of one-person, one-vote principle.	Extremely easy, particularly with military vote where commanding officers have significant power and influence over subordinates.	It is a court martial offense for a military officer to use their position to influence a person's vote. Voting Assistance Officers throughout the military help educate officers of the need to not influence voting. Criminal penalties are a disincentive	Leaders or personnel in positions of power or influence over a group can offer incentives for voters to vote in a particular way. Lack of oversight offers easy way for voting to be monitored by those who wish to do so. No way for voter to later spoil their ballot or change their vote. Offering positive bribes for voting in a particular way could be much more effective and less likely to be reported. Similarly, for non-military voters, easy for an individuals in some situations to force another individual to vote as the attacker pleases.	The potential for coercion is the result of absentee voting, where ballots are cast outside the protected environment of the polling place. By-mail voters can contact LEO to have the coerced ballot invalidated, but given potential transit time delays this might be infeasible for many UOCAVA voters.	Voter requests that LEO spoil cast ballot spoiled and requests new ballot. In this way a coerced voter, once outside the control of the coercer, could access another PC and vote their ballot. The absence of mail transit delays make this mitigation more viable for Internet voting.

Threat	Skill Needed	Consequences	Realistic	Countermeasures	How it happens in the paper by-mail system	Comments	How SERVE mitigated threat
Inserting fake voters	Medium	compromise of election	Some attacks require inside information; others can be done with creative and resourceful people of moderate skill; can be launched from anywhere	Investigate duplicate voter registration attempts to detect possible patterns of fraud. Criminal penalties are a disincentive	Attacker obtains list of registered voters in area they want to compromise as well as lists of people of voting age who are not registered. This can be done by infiltrating campaign that can obtain this information or by hacking into voter registration system. Easiest scenario is for attacker to cross-check list of registered voters with list of those who are of voting age to compile a list of those not registered. Attacker then submits FPCA for these voters (using their correct address for residence from phone book but an address of attacker's choice for UOCAVA address). Attacker then submits many ballots using these stolen credentials. This is even more likely in an era of significant military deployment. Slightly more difficult is to obtain list of registered voters by hacking into voter registration system, then selecting voters who have not voted for some period (obtained through VR system voter history file) and filing FPCA forms for them.	While HAVA requires ID for first-time voters who register by mail, UOCAVA voters are an exception. No proof of UOCAVA status is required, just voter affirmation; any person willing to perform such an attack will not be dissuaded by affirmation. Risk to attacker is that someone for whom they submit an FPCA also registers to vote. However, that would not necessarily enable LEOs to discern valid FPCAs.	SERVE required two approval steps for voting. First a voter's ID must be authenticated, either by appearing in person and presenting an ID to a trusted agent, or by using a military common access card (all of which are issued after a similar in-person authentication). Second, the voter must complete an application and be approved to vote by the LEO. This two-step process makes voter registration fraud harder to accomplish in SERVE than in the paper-based system.
Incorrect voting produces errors in ballot	Low	Disenfranchised voters	Highly likely	Improved instructions Simplified ballot designs	Voter can mark their ballot incorrectly (by circling chosen candidates name instead of connecting a line or filling in a dot), over-vote (selecting more candidates for a race than allowed in that race), or skip races --- resulting in an intended vote not being tabulated. .	Absentee voters using paper-based ballots cannot take advantage of error checking technologies (these are increasingly found in precinct voting systems).	Similar to DRE machines, SERVE prevented a voter from marking their ballot incorrectly thus preventing overvoting. SERVE would not have given voters option to incorrectly mark their ballot (circling names instead of connecting lines). SERVE would have prompted voters when undervote was possible

Threat	Skill Needed	Consequences	Realistic	Countermeasures	How it happens in the paper by-mail system	Comments	How SERVE mitigated threat
Incorrect completion of absentee ballot leads to ballot rejection	Low	Disenfranchised voters	Highly likely	Improved instructions Simplified and streamlined rules	Absentee voters can make common mistakes on the envelope containing their ballot --- they can forget to have the ballot witnessed (where required), to sign the ballot, or may make mistakes in providing address.	This is a potentially widespread problem for absentee voters using paper-based voting systems	SERVE would mitigate such problems by making sure that necessary fields are completed before ballot submitted; could undertake simple checks on validity of provided information.
Ballots intercepted while in transit	Medium	Disenfranchised voters	Illegal in many postal services but could be done by insiders or with foreign government collusion	Can mitigate risk with careful control of postal service personnel; harder to control once mail is outside US control; attack likely to go undetected Criminal penalties are a disincentive in jurisdictions where they apply	Could be easily done by U.S. or foreign postal service personnel, who can detain or destroy absentee ballots on their way to or from a voter. Attacker can easily detain ballots long enough for them to be received too late to be cast on time without risk of being caught or prosecuted. Most easily can be done to large groups of ballots in central mail facilities in countries with large US military or foreign service presence. Outside attacker could bribe postal personnel to detain or destroy ballots.	An organized interception of UOCAVA ballots would be high-risk endeavor if detected, but has little potential to affect the US election given the very small numbers of UOCAVA voters in any one country. No such attacks have been detected in the past, perhaps because antagonists may not view the risks as worth the limited potential gains.	SERVE would have supported a small fraction of the UOCAVA population; further reducing the chances that disruption of SERVE votes could affect an election.
Spouse or family member completes ballot and forges signature	Low	Disenfranchised voter, vote fraud	Occurs today	Limited. LEOs would need to check every signature against records. Good forgeries undetected	Spouse of family member intercepts ballot, completes it and returns it without the voter's knowledge. Voter believes that ballot never arrived. LEOs, with thousands of absentee ballots to review, generally cannot perform close reviews of voter signatures against records.		Voter would be sent an email if their ballot was cast. A voter who did not cast the ballot would be alerted to investigate the problem. Voter could also check SERVE and could see that their ballot had been received. Finally, voters educated about SERVE system would not believe that their ballot never arrived since there are no mail transit delays in SERVE.

Threat	Skill Needed	Consequences	Realistic	Countermeasures	How it happens in the paper by-mail system	Comments	How SERVE mitigated threat
Visually impaired voters cannot complete a ballot	Low	Person assisting a blind voter could change their vote	Possible	None – consequence of paper voting technology	Blind voters completing a paper ballot need assistance to read the choices and mark the ballot. The assistant could easily change the choices without the knowledge of the blind voter.		Blind voters could use software that can read web sites (e.g., JAWS) to read and complete their ballot in private in SERVE system. Many visually impaired voters who use the Internet already use such software routinely.

For SERVE, one critical security element was that SERVE would have required digital signatures for identification and authentication of all users. These signatures were X.509 medium assurance digital certificates capable of being accessed from any SERVE system-compliant browser anywhere in the world. SERVE compliant browsers included: Microsoft Internet Explorer, version 5.X and above; Netscape Navigator, version 6.1 – 7.0 (SERVE did not support Netscape 7.1). These browsers are capable of handling Secure Sockets Layer 3 (SSL3) encryption.

- Provide strong voter and LEO authentication for all processes.
- Trust no single entity to control everything, e.g., separation of logical and physical access, distribution of duties and authorization. (Alternatively, distribute trust among as many persons as possible.)
- Provide ability to validate software functionality before each use (e.g., 3rd party hash comparisons against escrowed copy).
- Demonstrate consistency of system operation by performing pre-, during and post-election system verification
- Provide robust fault detection and graceful degradation.
- Minimize chance that voter is fooled into presenting credentials to the wrong party or voting at the wrong site (spoofing).
- Minimize net side effects on the voter's computer (e.g., no persistent cookies, no data remnants).
- Discourage voter coercion and vote selling.
- Minimize additional security risks to the voter due to making his computer a more valuable target.
- Disenfranchise only a small number of voters due to virus, hacking, other electronic malfeasance (limited to isolated random events, not a systemic attack).

It was determined early in system development that medium level assurance was required to provide an appropriate degree of security for voter identification. Medium level assurance is defined in the Federal Bridge Certification Authority (FBCA) Certificate Policy (CP) as being relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Medium level assurance requires that any user of the system must have an initial face-to-face contact to validate identification. Once enrolled, the user would be authenticated every time he/she logs on to the system.

All system users (for example, eligible citizens, election officials, system operations personnel) were required to obtain digital signatures. For citizens, the key component of the enrollment process was the verification of a citizen's identity. A citizen's identity would have been verified through one of two processes: (1) validation by a Department of Defense (DoD) Common Access Card (CAC), or (2) validation by a Trusted Agent (TA). The DoD CAC is issued after an initial face-to-face identification to all active duty and reserve military, DoD civilians and DoD contractors working at a DoD facility. The CAC process is available for CAC holders who have access to a workstation equipped with CAC software and a CAC reader.

The second process would have been validation by a Trusted Agent (TA). TAs would have been individuals, authorized by FVAP and affiliated with approved organizations, who would perform identification (ID) proofing of citizens enrolling for a digital signature.

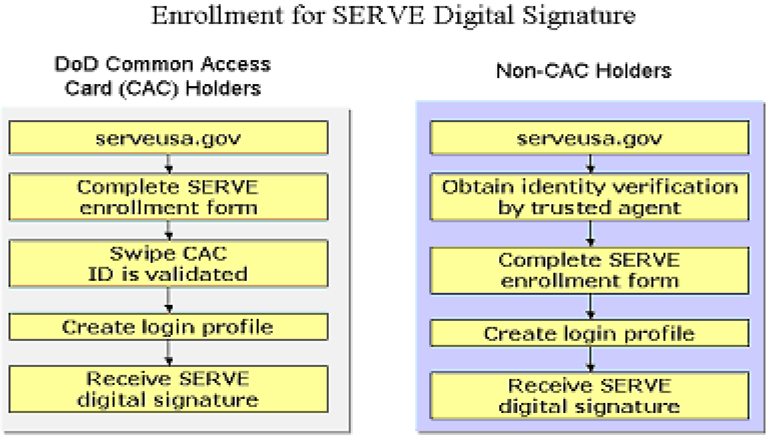
Enrollment for SERVE Digital Signature
DoD Common Access Card (CAC) Holders
serveusa.gov
Complete SERVE enrollment form
Swipe CAC ID is validated
Create login profile
Receive SERVE digital signature
Non-CAC Holders
serveusa.gov
Obtain identity verification by trusted agent
Complete SERVE enrollment form
Create login profile
Receive SERVE digital signature

Figure 4.1: Enrollment for Digital Certificates

SERVE's goal—because of the mobility of UOCAVA, especially military, voters—was to enable anyone to access the system from any workstation connected to the Internet. The Identification and Authentication (I&A) technology used to accomplish this were based on VeriSign's Roaming Service and Managed PKI (Public Key Infrastructure) Digital Certificate technology. This is a system of registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

All users of the system were required to be authenticated to the system. The Identification and Authentication (I&A) subsystem of SERVE system would validate a person's identity for the purpose of granting them access to the system. Once the authentication process was complete, the person's digital signature (A digital signature is a form of electronic identification granted to a user after the user has completed the enrollment process) would be available for use.

The VeriSign Roaming Service enables enterprises and consumers to securely download private data and digitally sign transactions, using digital certificates as credentials, from virtually any Internet-enabled personal computer (PC) or device in the world. SERVE was to have used this technology; however, a Certificate Policy (CP)/Certification Practices Statement (CPS) were specifically developed for use of this technology by SERVE. This technology was important for the SERVE system, because end users could easily execute secure transactions anytime, anywhere instead of being limited to a particular password-protected or smart card-equipped terminal.

Specifically, this Roaming Service provided the following features:

- It was easy to use, with access available from any personal computer/workstation, at any time, and anywhere with either Internet Explorer or Netscape browsers

- It was cheaper relative to systems requiring hardware devices

- It provided strong encryption and key information by storing the data on multiple physically separated servers to protect the digital certificate from unauthorized access by both external and internal sources

- The transactions were validated and stored so an electronic record of certificate use is always available.

4.1.1: Minimizing Other Threats

The goal of disenfranchising no more than a small number of voters due to virus, hacking, and other electronic malfeasance (limited to isolated random events, not a systemic attack) was and should be one of the most sought after goals of any distributed voting system such as the SERVE system. This goal is also one of the hardest to attain as the voter's systems were beyond the reach of the SERVE administrator's control. The SERVE design incorporated a number of checks in order to mitigate the risks posed by the inability to attain complete control of the remote voting platform. These checks were aimed in part at helping the voter to defend themselves against the potential for attacks on their computer, by either protecting their computer or by making vote tampering more detectable by the voter so the voter could take remedial actions.

For example, SERVE was designed to give the voter opportunities to verify that their vote was being recorded correctly. The vote summary page was returned to the voter as a picture file overlaid on a background graphic. The integration of the voter's choices and the background graphic in a centrally-generated picture file was designed to be difficult for an attacker to faithfully replicate with the voter's choices, improving chances that the voter would detect that something was amiss. The picture also included a Turing test with centrally generated content that a workstation attacker could not know in advance. These tests ask the user to type a simple word or phrase as it appears on screen, thus differentiating the user from an automated device. Voters who could not pass the Turing test would be asked to move to another computer or otherwise seek assistance (such as contacting the SERVE Help Desk.)[10]

If after voting, a voter discovered that their machine or vote had been compromised, SERVE provided a means for the LEO to spoil that ballot and give the voter an opportunity to cast a replacement ballot, presumably on an uncompromised machine. We should note that some of the participating SERVE jurisdictions were not planning to offer the ballot-spoiling feature, as they were uncertain of its legality in their states.[11] Once a voter cast their ballot, SERVE would send an email to the address provided when the voter enrolled in SERVE (based on an in-person verification) confirming that their vote had been cast. This communication provided an out-of-band communication that could alert voters to the unlikely event of their credentials being stolen.

[10] The Turing test could be a barrier for certain visually impaired voters. In order to avoid disenfranchisement of these voters, SERVE included a method that enabled LEOs to designate specific voters as exempt from the Turing test.

[11] It appears that State laws do not provide for ballot spoiling of cast absentee ballots partly because such a procedure would be impractical with paper by-mail ballots. In the by-mail system, it would be difficult to find the ballot to spoil, physically distribute the blank ballot replacement, receive the cast replacement, and ensure that no duplicate ballots are counted. As designed, the SERVE system removes these physical constraints, providing election officials with practical new options to improve the voting process. The ballot spoiling capability especially offers new methods to deter absentee voter coercion, as we will describe later.

The implementation of an Internet voting system inherently makes voter computers a more valuable target to those interested in affecting the outcome of an election. SERVE's main response to this security principle was to make the voter's computer harder to find by implementing a design that makes nearly all personal computers worldwide potential voting machines. In this way, many strategies to attack SERVE required an attack on all computers worldwide, including those set out by security companies whose business is to monitor for such attacks. The SERVE team viewed this as an advantage over a kiosk-based strategy which offered a much for focused target for potential attackers.

4.1.2: Data integrity, system transparency and accountability (audit logs, encrypted data, checking software hash codes, separation of duties, configuration management)

An imperative goal for a registration and voting system is the complete integrity of all data and the ability to audit that data. The SERVE system was developed to insure the integrity of all data and procedures. All information in the system would have been encrypted (as discussed in the section of this report regarding system security). As Table 4.4 shows, provisions were made to insure the physical security and integrity of the SERVE system, as well as all information that would be generated during use of the system by UOCAVA citizens and participating LEOs (again, the physical security measures are discussed in the section on system security).

The SERVE system would have generated enormous quantities of logging data that would be retained, at the most basic level possible. The system logging data would have allowed for post-election auditing analysis of all system functions, ranging from those performed when during the identification and authentication process, to the registration and voting process, and finally to all of the election administration processes allowed in the SERVE system.

4.1.3: Parallel monitoring or election validation testing

Once the SERVE system was implemented, there were plans to engage in a series of widespread tests of the system while it was operational. The first plan was to test the security of personal computers that would be voting on SERVE, and the second was to create hypothetical voters to collect usability data and to determine if hackers attempt to manipulate the SERVE system.

One question that arises in regards to Internet voting systems generally is the security of the voting platform used by the voter. This is the one part of the security architecture that neither the SERVE system—nor any other Internet voting system—can easily control with any degree of certainty. The relative insecurity of citizen computing platforms is a constant criticism of Internet registration and voting projects, and is a question that arose during the security evaluation of the SERVE system while under development. The development team approached this problem with so-called "social engineering" solutions, and was planning on providing system users with information about potential security problems on their computer, and possibly links to software that the system user could download to check their local computer for viruses, or to install firewalls, or other types of security software.[12]

[12] There have been solutions proposed for securing the voting workstation; for example, the California Internet Voting Task Force report recommended that election officials provide to remote Internet voters a unique operating system and

Most discussions of the security of Internet voting focus on “Internet-general” threats to the voter’s computer workstation. In other words, the voter’s workstation could be infected by the usual viruses that attack Windows-based computers, or by the “spyware” that is often inadvertently downloaded to workstations as users surf the web. There has been less discussion, however, of what might be called “SERVE-specific” threats to a voter’s workstation.[13] For example, malicious virus code that might have been downloaded if a SERVE participant visited a specific Congressional campaign website, or a certain party’s website, that would infect their local workstation and alter their interactions with the system in certain ways specific to their county ballot.

A series of tests for these potential vulnerabilities were under consideration:

1. Establishing a cluster of Windows-based computers with various security configurations. For example, some computers might be set up with high levels of security (all software updates, firewalls, and virus scans on full detection) and some with little security (no software updates, for example). These computers would be hypothetical SERVE voter workstations.

2. Development a web surfing protocol, where these hypothetical SERVE voter workstations with various configurations surf various websites on a regular basis. Some computers would surf prominent websites to obtain data on the background rate of security attacks on these workstations.[14] Others could surf websites that we assumed SERVE voters from certain counties might visit, like the county election website, the state’s website, political information websites for that area, and the websites of parties and candidates from the county. A third group of computers would have surf both prominent Internet and more UOCAVA voting related websites. Having the hypothetical voter workstations target different types of websites might allow the evaluation team to determine whether Internet-general or SERVE-specific threats are more predominant.

3. Last, use the logging function on the firewalls and virus scans, or employ software that has been developed for precisely this type of security evaluation, to measure and monitor what viruses, malicious code, and other security threats are encountered.[15]

Other permutations of these security evaluations were under development. For another example, preliminary work was underway on the deployment of a rudimentary “honeypot” (using either

web browser software to prevent virus or Trojan Horse software attacks on voter workstations (California Internet Voting Task Force Report, January 18, 2000, http://www.ss.ca.gov/executive/ivote/). One possible implementation would be providing each voter with a cd-rom; the voter would boot their workstation off this cd-rom, and the cd-rom would temporarily install a new operation system that would be used only for voting; when voting is complete, the voter reboots the system and their previous operating system is reinstalled.

[13] See SERVE Evaluation Team Memorandum 11, “Comments on Threat Assessment Report”, 4-11-2003.

[14] See http://www.google.com/press/zeitgeist.html.

[15] See Lance Spitzner’s recent book, *Honeypots: Tracking Hackers* (Addison Wesley, 2003). The “Honeynets project” (http://www.honeynet.org) provides a shareware software product, called “Sebek”, that measures and monitors activity on “honeypots” and “honeynets.”

shareware or commercial software) that would only measure background intrusion attempts, and on the eventual deployment of workstations in typical situations (workstations which would be on a computer network, with some security precautions, like firewalls and virus scanning) which would be used as outlined above to surf to websites that we would expect SERVE participants to utilize. By comparing intrusion attempts between the two types of workstations it might have been possible to analyze attempts to target the SERVE system.

A key methodological issue, however, with these approaches to measuring security threats for an Internet registration and voting system, was that the underlying incidence of security threats to the SERVE voting system is difficult to gauge before the fact. In other words, it was difficult to estimate the signal-to-noise ratio in this situation, or to know before the fact how many hypothetical voter workstations we have been necessary to detect a certain, quite low, level of security threat. This is an issue that requires additional research.

The second methodology that was being developed to provide for parallel testing was the development of hypothetical voters. As the evaluation team and participating LEOs would have logged every action that the hypothetical voters undertook, if there were any attempts by hypothetical voters generated for parallel testing to access the system outside the evaluation/LEO tests, this would be evidence that some effort to penetrate the SERVE system security were underway. In fact, it might have been possible to use the "honeypot" UOCAVA voter workstations discussed earlier as platforms from which selected hypothetical voters might access the SERVE system; this would have allowed for the correlation of the detection of activity on the SERVE system by the hypothetical voters with the log of actions undertaken by those hypothetical voters on the "honeypot" workstations—as well as the possible detection of how outside actors were able to obtain the identities of the hypothetical voters and their authenticating information.

4.2 Process Design Principles

- Deliver correct ballot style to voter.
- Ensure a secret ballot, i.e., no association of voter with ballot choices.
- Ensure that only one ballot counted per voter.
- Provide reliable vote transport and storage.
- Preserve voter preferences unchanged throughout the entire process, from initial selection through tabulation.

4.2.1 Accuracy and verifiability in voter registration

As discussed earlier, the first step of the absentee voting process for UOCAVA voters using the existing by-mail process is voter registration. Different jurisdictions have different requirements for valid voter registration information, and in the past a frequent problem with UOCAVA registration applications has been inaccuracies in voter registration applications. Registrants often make simple errors that invalidate their FPCA. For example, voters will:

- Provide a post office box, not a physical street address, for their home address.
- forget to sign or date the registration application, or

- write with poor handwriting, making one or more critical fields illegible.

In any of these cases, the registration request may be rejected with insufficient time to communicate with the citizen, resulting in the citizen not receiving an absentee ballot for that election.

The SERVE system was designed to facilitate accurate and timely voter registration, and to alleviate or eliminate these typical problems that UOCAVA citizens face when they try to register and request an absentee ballot. Once the UOCAVA participant was granted access to the SERVE system using their digital certificate, they could then access the voter registration application in SERVE system. The SERVE system voter registration application would have been established to assist UOCAVA citizens to register in their jurisdiction; the electronic voter registration application checked the required fields and did not allow submission of the form until data was provided.

The electronic delivery of the voter registration application directly to the appropriate LEO database would provide election officials with instant access to the registration applications. Upon receipt, the LEO would then undertake their normal procedure to authenticate and validate the UOCAVA citizen's eligibility, and would then update the SERVE system that the citizen was either eligible to vote (and which ballot style the citizen should receive) or not. If the citizen was not eligible, then a reason had to be entered. This decision would then have been made immediately available to the UOCAVA citizen, who could use the "check status" feature of the SERVE system to determine whether their voter registration request had been received by the LEO and what the LEO's action on the request had been.

In cases where there was a problem with the application and the LEO did not immediately register the UOCAVA citizen, that decision would have been communicated to the citizen quickly, allowing the citizen to try to register again electronically. Since the application captured the email address, the electronic medium also gave the citizen and LEO the opportunity to contact each other, allowing for the rapid resolution of registration application problems.

It is also important to note that the electronic nature of the registration system means that many of the problems associated with FPCA rejections in the by-mail process such as illegible writing and failing to complete all fields in the form can be eliminated.

4.2.2 Delivering correct ballot style to voter (control data)

Guaranteeing that each voter receives the correct ballot for their specific voting jurisdiction is a difficult problem for election administration. The SERVE system would have allowed for a high degree of accuracy in correct ballot provision. Once a voter was registered to vote using the SERVE system, the LEO would designate which ballot style that voter should receive. Once that ballot style was inserted into the system, it would have been provided only to those UOCAVA voters who should receive the specific ballot. Assuming that correct ballot style information was provided to the SERVE system, there would have been a very high degree of accuracy of ballot provision to UOCAVA voters.

4.2.3 Ensuring ballot integrity (ballot formatting, review and signoff, ballot logic)

There were two methods for LEOs to provide their ballot styles to the SERVE system: (1) the "service bureau" or (2) the direct use of ballot definition software available as part of the LEO side of the SERVE system. In the "service bureau" process, LEOs would provide their ballot styles to the SERVE development team, who would then develop the necessary electronic ballots for the jurisdiction. This would have mirrored the current process where LEOs provide ballot information to a printer, who creates ballots and provides the LEO with ballot "proofs" and then final ballots. In the direct use of the ballot definition software, the LEO itself would provide the ballot logic and information, and would have a variety of procedures and processes to check the validity of the ballot styles.

4.2.4 Accurately capturing voter intent and voter ballot verification

The SERVE system was designed to minimize simple errors that voters can make, and to give them an opportunity to verify that their ballot was received by their election official. By providing a web-based voting experience, the SERVE system would have allowed election officials to incorporate their "election logic" directly into their electronic ballots. Voters could only cast ballots for races that they were eligible for, could not have cast more votes than possible for a particular race, and would have been prompted for verification in cases where the voter did not cast a ballot in a specific race. These features would have allowed UOCAVA voters to avoid the common problems of over- and under-voting, thus potentially allowing them to cast ballots that would have been more closely consistent with their intentions than under the existing paper-based by-mail system, which does not provide any convenient and simple way for the voter to verify that their intentions are being recorded accurately.

Additionally, the SERVE system had two features that would have helped UOCAVA citizens verify that their ballot was received by the appropriate election official. When done with the balloting process, the UOCAVA citizen would have clicked on a "button" in their electronic ballot reading something like "Vote" or "Submit Vote". This would have initiated a series of behind-the-scenes actions; primarily the transmission of the ballot to the SERVE voting engine. The voting engine would have provided the voter with a summary of their ballot for review, noting the voter of the races where they failed to cast a vote. At this point the voter had an opportunity to verify their ballot. Additionally, at this stage the voter would also complete a Turing Test, and then digitally sign their ballot. The verified and digitally signed ballot would then be sent as an encrypted object to the SERVE system, which would then notify the appropriate election official that the ballot was ready for reconciliation, downloading, decryption, authentication, and possible tabulation.

Last, the SERVE system would have provided UOCAVA citizens various opportunities to check their status on the voting system. Prior to voting, the UOCAVA citizen could check their registration status, and also check their ballot availability. After casting their ballot, the UOCAVA could verify that the local election official had received the ballot. To provide additional security where allowed by state law, UOCAVA participants would have been able to utilize a non-Internet based procedure to invalidate their returned ballot and to obtain a replacement ballot.

4.2.5 Maintaining ballot secrecy

As the SERVE system was modeled upon the existing absentee voting process, there always existed the possibility that a UOCAVA citizen could have their privacy violated while voting (for example, by having to use a workstation in a public place to vote) or to have been coerced into casting a ballot that was contrary to their intended vote. Given that the existing absentee voting process was the design framework for the SERVE system, there was little that could be done to increase the basic privacy of the balloting procedure, relative to the existing vote-by-mail system.

However, relative to some of the methods that UOCAVA citizens have used in recent elections to cast their absentee ballots, the SERVE system might have allowed for a higher degree of privacy and secrecy. This is especially the case when the SERVE system process is compared to the use of facsimile machines (fax) by UOCAVA citizens to return their ballots to election officials. The return of voted ballots via fax are inherently sent unencrypted over telephone lines to the election official, and the voter relies on the integrity and professionalism of that official. The SERVE system would have mitigated or eliminated many of these privacy and security concerns.

Last, UOCAVA citizens participating in the SERVE project could have used an "out-of-bandwidth" method to invalidate their returned ballot and to have potentially obtained a new ballot to vote. This process would have allowed SERVE participants to receive a new ballot in the eventuality that they were coerced into casting a ballot, or in situations were they were not convinced that the original ballot had been received by the appropriate election officials. This process may also have helped foil "vote buying" schemes, as a UOCAVA citizen participating in the project could have voted the ballot the "buyer" desired, but since the buyer would never know if this was the citizen's final official ballot, would not approach the voter in the first place.

4.2.6 One vote counted per voter

The SERVE system would have allowed each registered voter to cast only one ballot through system notifications to the LEO and the use of procedures already in place in local election offices with the by-mail process.

4.3 Usability Design Criteria

- Comply with accessibility requirements of Section 508, 29 US Code (USC) 1794d.
- Enable voter confirmation of ballot choices as recorded by system.
- Ensure that recorded ballot choices match voter intent.
- Minimize cost to voter (try to avoid special hardware or software).
- Maximize system availability throughout voting period.

4.3.1: Usability for Special Populations

Section 508 of the Rehabilitation Act (29 USC) requires that electronic and information technologies that are provided by the Federal government be fully accessible to people with disabilities. As applied to the SERVE system, Section 508 required that the SERVE system be accessible to participants who were blind or vision impaired. The SERVE system was designed to so that screen reader programs (like "JAWS®") could operate and that UOCAVA participants with vision impairments could have had the voting information on the screen read aloud to them.

The federal Voting Rights Act requires that election jurisdictions that meet the following criteria to provide balloting materials to individuals in minority language groups, in addition to providing the balloting materials in English. A covered jurisdiction is a covered State or political subdivision that, based on Census data, has:

- more than 5 percent of the citizens of voting age that are members of a single language minority and are limited-English proficient;
- more than 10,000 (voting age) citizens of a political subdivision are members of a single language minority and are limited-English proficient; or
- in the case of a political subdivision that contains all or any part of an Indian reservation, more than 5 percent of the American Indian or Alaska Native citizens of voting age within the Indian reservation are members of a single language minority and are limited-English proficient.

Additionally, the illiteracy rate of the citizens in the language minority as a group must be higher than the national illiteracy rate.

Because several covered jurisdictions were to participate in SERVE, the provision of multilingual ballots was a feature that became part of the SERVE system design. The system was designed to allow for multiple languages in the ballots delivered to citizens, with this capability embedded in the ballot design process thus allowing any jurisdiction to create ballots in any languages required. For states that did have multiple language ballot requirements, the citizen would have been prompted to choose a language. The blank ballot delivered to the citizen would be in the chosen language.

Of the states and counties that were participating in SERVE, Hawaii and Florida had multiple language requirements. In Hawaii, there are counties where ballots must be available in Chinese, Filipino or Japanese, as well as English. There are Florida counties that have to be able to provide ballots in Haitian Creole, Spanish, and English. Although the SERVE web site, www.SERVEUSA.gov, was only in English, links were provided to each state's election site and many of the county election sites. Where required, these state and county election sites contain information in multiple languages.

4.3.2 Help Desk and Other Usability Features

In addition to legal accessibility issues, it was also critical that the SERVE system meet the usability needs of both UOCAVA voters and LEOs. Various means were established to study and evaluate the usability of the system. First, during the development of SERVE system, usability experts provided substantial input and critical analysis of the usability of the system. This usability evaluation would have continued in parallel with the development of the system before implementation. Second, after implementation, a variety of measurement strategies were ready for obtaining usability information regarding the system: these included exit surveys of UOCAVA participants, post-election interviews with LEOs, collection of detailed system logging information that would have tracked interactions with the system for UOCAVA participants and LEOs alike (and errors made), and the retention of logs from the "help desk".

Information that was to be logged from the system included attempts to get system assistance (for example, when users clicked on help buttons); voting registration information (for example, the number of times the user changes VR information); identification and authentication (for example, logs of when trusted agents signed proofing messages); election administration (for example LEO logons); ballot definition logs (when LEOs created the ballot for an election); voting (for example, when a voter failed the Turing test); and last, logs from VeriSign (for example, the number of attempts by a user to obtain a digital certificate). In sum, an enormous quantity of information was to have been collected from SERVE system logs that would have allowed detailed tests of system usability. The following data were to be captured from the "help desk", and used to evaluate system usability.

4.4 Auditability Design Principles

- Deliver correct ballot style to voter.
- Ensure a secret ballot, i.e., no association of voter with ballot choices.
- Ensure that only one ballot counted per voter.
- Provide reliable vote transport and storage.
- Preserve voter preferences unchanged throughout the entire process, from initial selection through tabulation.

4.4.1: Logic and Accuracy Testing

The development and evaluation teams worked on procedures to test the integrity of the SERVE system itself. The typical practice in the election administration field is for administrators to conduct pre-election, and sometimes post-election, "logic and accuracy" tests of their voting systems. The rationale for such tests is to ensure that all possible vote combinations can be read accurately by the tabulation software. One way these tests are conducted is by setting the voting system into "test mode", and for the administrator to create "test voters", in "test jurisdictions", and to run a "test election." As the administrator knows exactly how the test election should result, these mock elections are seen as an important tool to understand the integrity of the voting system.

Some criticize the use of voting system test mode for checking the integrity of voting systems. These criticisms have arisen in analyses of the SERVE system: if the system "knows" that certain voters are test mode voters, then an intelligent hacker (or a disgruntled employee) could disguise their attack by allowing the test mode function to operate correctly, while later being able to attack the real election with their malicious code.[16]

A number of novel ideas were developed during the SERVE project regarding this problem. Consider a hypothetical SERVE participant county. With the assistance of election officials from the participating county, a set of hypothetical voters could have been created. These voters would be authenticated and registered just as any real UOCAVA voter, and there would be no *electronic* indication that these are hypothetical voters. Record of the hypothetical voters would be retained off-line. These hypothetical voters would have then cast ballots, their balloting would be known, and their ballots would be tabulated separately during the election canvass. Any deviations between their known balloting, and the tabulated returns of their balloting, would be an obvious indication of some problem (what the nature of the problem was, and whether it was intentional or not, would then have to be determined with subsequent investigation). As there would be no electronic indication that these were test voters, it would be difficult or impossible for outside hackers to know the test status of these voters.

As it was unknown whether election officials would allow for the creation of test voters, and for their ballots to be mixed until after the canvass period with real voters, other novel methods of parallel testing were to be used during the implementation of SERVE system in the 2004 elections. One alternative method was to create hypothetical voters in a fictitious county in a SERVE participating state, a fictitious precinct in a SERVE participating county, or a fictitious SERVE participating state to determine if there were attempts to tamper with the voters in the dummy states, or the votes of these dummy voters once cast, or even the workstations used to cast these hypothetical votes.

In this test, a set of dummy voters would be registered into the SERVE system in the dummy jurisdiction. If the SERVE system were to be compromised, some of the hypothetical voters would be comprised as well. That is, if a vote were cast in the dummy jurisdiction, it would be known that the system had been compromised. Additionally, at the end of the experiment, some of these dummy voters could cast a fixed ballot and the results of these votes could be compared with the votes to ensure that the system integrity held. An important issue here is the statistical power of this test, or exactly how large the sample of test voters would need to be to adequately assess security threats. This would need additional examination if we were to proceed with one of these types of security measurement and monitoring studies.

Last, it is important to note that this methodology would also have provided an important source of usability data. If the test voters are real individuals, say at different universities throughout the nation, it would have been possible to study their reactions to the usability of the system. These usability studies would have provided additional, and possibly more detailed, evaluation of the SERVE system’s usability.

[16] These criticisms have also been leveled against precinct electronic voting devices. This has led jurisdictions to mandate the use of “parallel testing”, ideas that are analogous to those discussed here. A “parallel test” procedure for precinct electronic voting devices involves taking some randomly sampled set of these devices out of use (without any advance notice to all but a few election officials in the jurisdiction), then thoroughly testing the integrity of vote recording for these randomly selected test voting devices. As the SERVE system would not utilize any voting devices itself that could be tested, and as registration and voting would have occurred over a period of weeks, straightforward application of current “parallel testing” methodologies in the SERVE setting was not possible.

4.4.2: Results reporting, results merging and combined summaries

As part of the election administration component of the SERVE system that LEOs could access, there was a module allowing the LEO to generate a variety of reports based on the UOCAVA activity through the SERVE system. The goal was to allow LEOS to generate all of the necessary reports for their administrative procedures, and for LEOs to have simple ways to incorporate electronic information from these reports into the existing administrative applications. LEOs would have been able to log into the election administration applications, and generate reports for:

1. Submitted applications
2. Applications pending information
3. Approved voters and precinct identification
4. Rejected applicants
5. SERVE drop-outs
6. Precinct to ballot style associations

This application would allow the LEO to generate a report for each of these topics, and the report could be saved and downloaded in comma-delimited format so that it could be easily integrated into other election administration applications that the LEO used for absentee balloting, tabulation, and report generation.

4.4.3: Provisions for recounts

All information that LEOs would access for their UOCAVA registration and voting tabulation would be retained for the purpose of conducting post-tabulation recounts, either mandatory or discretionary. Additionally, all system logging data could be used for the purpose of detailed post-election auditing and accounting purposes.

5: System Accreditation and Certification

The certification and accreditation process for the SERVE system differed significantly from that applied to voting systems, for a variety of reasons.

- The SERVE system was designed as an integrated system performing voter registration, voting, vote tabulation and other functions. While the applicability of the Federal Election Commission (FEC) 2002 Voting System Standards (VSS) to the voting and vote tabulation functions was clear, there are no standards or accreditation process defined for voter registration and other functions.

- The SERVE system was an Internet-based system and subject to different operating modes and access methods than conventional software-based voting systems. It contained components and features that were not anticipated in the VSS. Therefore, the standards and accreditation process for these components and features was not defined, nor was there significant precedent on how to apply the VSS in this circumstance.

- The SERVE system processed sensitive information and therefore should go through a security certification and accreditation process. However, the standards and process for this are not well defined. Compliance with the DoD security regulations is not mandatory for SERVE because it does not store or process any DoD information. Rather it processed sensitive data on behalf of the participant states. Since SERVE was built within the DoD framework, and because the DoD has mature, well-defined processes and standards for security certification and accreditation, FVAP elected to use the DoD security certification and accreditation process as a model for development of the certification evidence. The accreditation decision, however, rested with the participant states.

Because of these factors, the certification and accreditation process was carefully defined to comply with the VSS, where applicable, and to follow the spirit and intent of policies and best practices in the less well-defined areas. Another significant difference in the SERVE accreditation process was the involvement of FVAP in the oversight of the activity. Normally, the voting system developer contracts for, and provides guidance to, the independent tester. There is no involvement by election officials, who are the ultimate system users. In this instance, FVAP contracted for independent testing services and was heavily engaged in the oversight of the effort. FVAP also consulted with state certification officials and other election officials regarding the certification process.

FVAP used a competitive procurement process to select an independent testing contractor to build the body of certification evidence needed for the States to accredit the SERVE system. The scope of work covered all functional and security aspects of SERVE:

- Certification of the voting system portions of SERVE using the FEC 2002 VSS;

- Independent Verification and Validation (IV&V) of system functionality in all other areas;

- Accessibility testing to determine compliance with Section 508 of the Rehabilitation Act.

- Security certification to verify that the system met all stated security requirements; and

- Penetration testing to evaluate the system's resistance to unauthorized access and abuse.

As required by the VSS, the contractor was certified by the National Association of State Election Directors (NASED) as an Independent Test Authority (ITA) for voting systems. In this role, the contractor supports the NASED to ensure that voting systems are reliable, accessible, private, and secure. The contractor performs this function using the 2002 Federal Voting System Standards, developed by the Federal Election Commission.

5.1 Certification Process Flow

The certification process, if properly executed, integrates with the overall system development effort so that compliance issues or unanticipated security flaws are detected early and can be corrected as easily as possible. The certification process consists of following steps.

1. The system owner (in this instance, FVAP working cooperatively with the participating states) will gather all relevant functional and security requirements for the system. These requirements can originate from voting system specific standards such as the Federal Election Commission Voting System Standards (VSS), state specific requirements, documentation requirements and requirements from other recognized sources. In the case of SERVE system, the following documents were drawn from: VSS, individual state requirements, ISO 17799, NIST SP 800-53, Open Web Application Security Project (OWASP), existing security relevant features in the design documentation, and generally recognized security best practices.

2. The system owner will create a comprehensive requirements document that identifies all functional and security requirements for the system and maps them to their source. For future use a requirements matrix (RM) should be created and populated with the requirements. Further along in the C&A process this matrix will become the requirements traceability matrix (RTM) and will assist in future steps to document how requirements are being met in the system. The RM is then provided to the system designer/builder and IV&V vendor. The following column heads represent minimum information for the RM (an example has been included):

Req #	Requirement	Source
1	Firewalls must be used	VSS 1.1

3. The system designer/builder reviews the system RM and ensures that it is consistent with the operational environment intended for the system and that all requirements can be met.

4. If any requirements can't be met by the system design/builder a request is submitted to the system owner for a revision or deletion of the requirement. The system owner makes

a decision on the system design/builder’s request for requirement revisions and/or deletions and issues an update RM if changes have been made.

5. The system designer/builder utilizes either the original RM or the updated RM if requirements were changed to design the system. In addition to the design of the system, all required documentation should be created for this step as part of the process.

6. The IV&V vendor creates test plans and scripts for all requirements submitted by the system owner in the RM. The test plans and scripts should be written to assess the compliance of the system against the RM. Each test case should be numbered and identify the requirement it is testing against, the objective of the test, assumptions and/or preparation steps, expected results, and the actual results. This information is later utilized in the RTM document as input into the compliance status of requirements.

7. The system designer/builder uses the system design to build the system while ensuring that all requirements from the RM are met. (Steps 7 and 8 should be completed in tandem).

8. The system designer/builder documents the system. (Steps 7 and 8 should be completed in tandem). Required documentation includes: System Security Plan, Risk Assessment, Security Feature’s User’s Guide, Trusted Facility Manual, Contingency Plan, Configuration Management Plan, and Operations Manual[17].

9. The IV&V vendor uses the test plans and scripts to test the operationally ready, locked down, system against the RM. A compliance report with all findings is created by the IV&V vendor and provided to the system owner. The compliance report includes the Requirements Traceability Matrix (RTM) with comments and assumptions by the IV&V and the compliance status for each requirement. The following column heads represent minimum information for the RTM (an example has been included):

Req #	Requirement	Source	How Requirement is met by system	Assumptions	Compliance Status
1	Firewalls must be used	FVSS 1.1	Checkpoint Firewall NG running on Windows 2003 Server.	Any general-purpose firewall can be used.	Compliant

[17] This list of documents is an example of how the SERVE certification process drew upon the body of knowledge within DoD for security certification practices. The documentation listed here is defined in terms of content and purpose by DoD security standards. As such, they are well known among both system integrators and security testing vendors. By using this common framework, the SERVE certification process leveraged DoD regulations even though they were not directly applicable to SERVE.

10. The compliance report is reviewed by the system owner and either accepted or rejected. If the report is accepted (compliance status is satisfactory to system owner's standards and the requirements for the system), the report is submitted to the National Association of State Election Directors (NASED). NASED will review the report and if accepted, will assign a NASED certification number. If the report is not accepted, steps 7, 8, and 9 are repeated until the report is accepted by the system owner.

11. The accreditation process varies state by state. For states that only require NASED certification, proof of the certification must be produced prior to system usage. Some states have expanded on the VSS for their voting system accreditation process; others do not. For states with their own requirements, the ITA would create a traceability matrix showing how the states requirements are met and cross-referencing this to the functional test results and assurance evidence collected during the certification process. For other states, they would be allowed to review the general certification evidence and the Requirements Traceability Matrix (RTM) to provide assurance that the system met all required functionality and was secure.

The remainder of this section discusses the process of SERVE system certification and testing, following the schematic given above. The following discussion also notes the rationale for the various decisions made during the certification and testing process, as well as how far along this process was when the SERVE project was halted.

5.2 Application and Interpretation of Standards

The overall system certification and accreditation approach selected by FVAP was designed to be broad in scope, covering standards compliance, functional testing, usability testing, and thorough security testing. The goal of the certification process was to obtain an independent body of evidence showing the system met all requirements. Before this could be achieved, it was necessary to determine how the various standards would be interpreted and applied to SERVE.

5.2.1 Voting System Standards

The FEC 2002 VSS provides certification standards for voting systems. The VSS was directly applicable to the voting portion of SERVE system, and as such was applied by the ITA, as it would be to any voting system. The interpretation of this standard was not entirely straightforward due to the difficulty in isolating the voting functions of SERVE system from the larger system and the presence of Internet-based communications. The certification process used by the ITA is described in detail below.

5.2.2 Software Independent Verification &Validation

Since SERVE system contained functionality that extended outside the boundaries of the VSS, an Independent Verification and Validation (IV&V) approach was used to apply the spirit and intent of the VSS as much as possible to other portions of the system. The IV&V process extended the code review process mandated by the VSS to include more thorough review and testing of the software.

5.2.3 Security Standards

As mentioned earlier, FVAP wanted to take advantage of the great body of knowledge that exists within the DoD regarding security standards and assurance testing. Even though DoD regulations were not directly applicable to SERVE system, many of the security standards in these regulations were used to create the SERVE system security certification approach. The security requirements for SERVE system came from several sources: the VSS, individual state requirements, ISO 17799, NIST SP 800-53, Open Web Application Security Project (OWASP).

The certification team also extracted security-relevant features from the system requirements and the system design documentation. Most, but not all of these were in the security section of the system documents. The team looked in other sections to find security-relevant items that were not explicitly labeled as “security” requirements. The certification team also proposed some security requirements for the system drawn from generally recognized security best practices and their experience with the types of security measures used in similar high-value systems. Each of these sources was reviewed and the relevant requirements were consolidated into a single set of security requirements that was used as the basis for certification.

It should be noted that SERVE system was unique in that it had a large number of features that could be considered both security features and application functional features. An example was digital signatures applied to voting transactions, providing voter authentication. These signatures were required as a functional part of the voting process. They also played a role in protecting the system from misuse and protecting the database from corruption. These “crossover” features were included in the scope of the security certification even though they were also tested as part of functional acceptance testing. The focus during security testing of these features was on their robustness in protecting the system against attack and abuse.

5.3 Overview of Federal Election Commission 2002 Voting System Standards Certification Process

The Voting Systems Performance and Test Standards document issued by the Federal Election Commission (FEC) April, 2002 defines how the ITA is to accomplish its mission.

This section outlines a process that implements the test requirements provided in the FEC 2002 VSS. It is not intended to be exhaustive as more detail is provided in various checklists and templates. Portions of this process are necessary for the execution of business by the ITA and are not found in the FEC Standard.

5.3.1 Technical Data Package and Source Code Review Process

This phase involves the review of the Technical Data Package (TDP) and Source Code. Both of these in-depth reviews are done using ITA templates, which map the FEC 2002 VSS requirements to an ITA checklist to verify completion of the requirements for those standards.

5.3.2 Technical Data Package Review

The Technical Data Package includes the following documents per the FEC 2002 VSS:

- System configuration overview
- System functionality description
- System hardware specifications
- Software design and specifications
- System test verify specifications
- System security specifications
- User/system operator procedures
- System maintenance procedures
- Personnel deployment and training requirements
- Configuration management plan
- QA program
- System change notes.

Each document is reviewed and functionality is mapped back to the FEC 2002 VSS. This is done using a review checklist.

5.3.3 Software Code Review

The software code is reviewed against the FEC 2002 VSS requirements. Those standards specify how the software should be written including naming conventions, restrictions of process flows, software design protections, as well as how the software should be documented. The standards are categorized under the following:

- Software Standards
- Software Sources
- Software Design and Coding Standards
- Selection of Programming Language
- Software Integrity
- Software Modularity and Programming
- Control Constructs
- Naming Conventions
- Coding Conventions
- Comments Conventions

The Source Code Review process also checks for embedded code, unauthorized changes, and complete documentation.

5.3.4 Pre-test Preparation

There are three pre-test preparation steps:

1. The developer makes available to the ITA all the hardware and software and test materials for the voting system that are required to perform qualification testing. System components include hardware, software, voter and operator manuals, maintenance manuals, program listings, facsimile ballots, tapes, and sample output report formats.

2. A meeting is held to finalize test schedules, review plans, and begin the qualification test process.

3. All hardware and software is setup and a system check is performed to ensure that all equipment and software are operating properly.

5.3.4 Qualification Test Plan

Qualification testing includes the following tasks:

1. The TDP Review which includes but is not limited to the checking the following:

    - Design standards and conventions used in the development of the vendor's software;
    - Specifications for the environment and interfaces;
    - Functional specifications;
    - Program architecture specifications; and
    - Test and verification specifications.

2. Defining the test plan procedures if the vendor has not provided them. The test plan and procedures are generated from the software requirements extracted from the FEC guidelines and the specific requirements obtained from the vendors documentation. If the vendor's module test case design does not provide conclusive coverage of all program paths, then the ITA shall perform an independent analysis to assess the frequency and consequence of error of the untested paths. The ITA designs additional module test cases, as required, to provide coverage of all modules containing untested paths with potential for untrapped errors.

3. Review of the Software Source Code for compliance with the FEC 2002 VSS for software quality and reliability. The review will also compare the standards set forth by the vendor in their own software specifications manual to the source code. The source code review includes but is not limited to:

    - Readability
    - Understandability
    - Modularity
    - Robustness
    - Security
    - Maintainability
    - Consistency
    - Documentation

- Usability
- Flow Control

5.4 Functional Testing Process

Functional testing is performed on each voting system software module as well as for the voting system as a whole. The main goal of the functional testing is to verify that the system performs all the features required by the FEC 2002 VSS as well as the TDP. Any anomalies discovered will be reported to the vendor in a timely manner in order for the vendor to correct the anomaly and re-submit the software.

5.4.1 System Testing

System Testing includes, but is not limited, to the following.

Volume tests – to investigate the system's response to processing more than the expected number of ballots/votes per precinct, or more than the expected number of precincts, or to any other similar conditions that tend to overload the system's capacity to process, store, and report data.

Stress tests – to investigate the system's response to transient overload conditions.

Usability tests – tests software responses to user input control or text syntax errors, error message content, audit message content.

Accessibility tests – tests system capabilities and features intended for use by voters with disabilities.

Security tests – designed to test (and try to defeat) the security provisions of the system including modification or disruption of pre-voting, voting, and post voting processing. This testing includes testing unauthorized access, deletion, modification of data, verifying including audit trail data, and testing modification or elimination of security mechanisms.

Performance tests – to verify the accuracy, processing rate, ballot format handling capability, and other performance attributes required by the system.

Recovery tests – designed to verify the ability of the system to recover from hardware and data errors.

5.4.2 Test Data Criteria and Recording Methodology

A matrix is used for mapping test results to the FEC 2002 VSS. The test is recorded as a pass or fail and there is space for comments. Test criteria are identified. Test criteria are what is to be measured and how tests and results are to be recorded. These criteria include, but are not limited to:

Tolerances - the acceptable range for system performance.

Samples - the minimum number of combinations or alternatives of input and output conditions that can be exercised to constitute an acceptable test of the parameters involved.

Events – the maximum number of interrupts, halts or other system breaks which may occur due to non-test conditions. (This does not include events from which recovery occurs automatically or where a relevant status message is displayed.)

The test results are recorded and are published as an appendix to the Final Qualification Test Report.

5.5 Final Qualification Test Report

Once all the FEC 2002 VSS requirements have been met and the voting system has been tested successfully, a final qualification test report is produced by the ITA. This report usually is delivered to the system vendor and to the NASED Technical Committee. This step happens after the initial system-level testing and includes a complete set of software that will become the qualification copy. In the SERVE case, this report would have been delivered to FVAP and to NASED.

Physical Configuration Audit

The physical configuration audit is done to verify the vendor's software development process with respect to design and development, software defect reduction, and change management. The ITA assesses the vendor's business capability to provide ongoing system support and software maintenance throughout the useful lifespan of the system.

Production Source Code Compilation

The ITA witnesses the build of the same source code that was submitted for the code review and testing. The build is witnessed as the software is compiled. During this step document versions are gathered, the source is compiled and built into an executable.

Generate Installation Package

The source code from the previous step is converted into an installation package and transferred to production distribution media. The resulting copy of source code and installation package becomes the qualification copy for the final system test and would be retained by the tester, FVAP and any state agencies requiring software escrow.

Final System Level Testing

The final system level testing is to assure that all known problems have been resolved and that the production installation package is complete and functional. The Qualification Test Procedures are used, but are used on the ITA qualification copy of the installation software package. Associated voting machine hardware shall be used as appropriate to provide inputs and/or outputs to the software under test. Problems encountered at this stage are reported to the vendor and (if applicable) retested. Recompilation of the production code may be required at the ITA's discretion. If required, Commercial Off-the-Shelf (COTS) functional and volume hardware testing is done in accordance with FEC Standards.

Final System Level Regression Testing

Regression testing is the process of testing changes to computer programs to make sure that the original functionality still works with the new changes. During the software development life cycle if software changes are made and tested, it is still necessary to test the whole system. Regression testing is a normal part of the program development process. Test department coders develop code test scenarios and exercises that will test new units of code after they have been written. Before a new version of a software product is released, these test cases are run against the new version to make sure that all the old capabilities still work properly. Regression testing is done to make sure that any software changes have not introduced errors.

5.6 Independent Verification and Validation (IV&V)

The Independent Verification and Validation process is well known in the software industry. This process provides an independent assessment of the system and ensures that it works. The verification and validation aspects of this process ensure through an assessment phase that a valid definition of how the software should work and then process into testing to determine if it does work.

The IV&V process for SERVE system was that all software that was not covered by the FEC 2002 VSS (for example, voter registration) was to pass through the IV&V process. The IV&V process starts with determining a standard of acceptable performance for each system requirement. By reviewing the SERVE system documentation and interviews with subject matter experts, a model of each functional portion of the system was developed.
An IV&V test plan would have been developed for each functional portion of the SERVE system and a testing case matrix created. The ITA would execute the test plan and all discrepancies would be resolved with the SERVE system development team. This process would be repeated if necessary until a successful test was accomplished. A major test case that would be added to the test plan was an end-to-end test of the system. This day-in-the-life test would be performed on the IV&V accepted software as well as FEC 2002 VSS certified software. This test would include backup procedures and other operational procedures. The IV&V process never progressed into the testing phase due to the termination of the project.

5.7 System Security Certification

As described above, the scope of the system security certification was broadly established. This was due primarily to the fact that security was considered by FVAP to be a critical success factor for the SERVE system, given the sensitivity of the voting process and the significant Internet security issues described earlier in this report. The ITA used standard Security Test and Evaluation (ST&E) compliance testing and penetration testing (also called "ethical hacking") techniques as the basis of its security certification approach. The ST&E portion is designed to ensure that all required security controls/features are both present and effective. Penetration testing evaluates the system's resistance to common forms of attack and misuse through hostile test techniques (i.e., attempts to break or bypass the system's security controls).

The ST&E compliance testing activities were structured to test all required and proposed security-relevant features and provide assurance evidence that each security feature mentioned in the security requirements traceability matrix is actually present and effective in the operational system. The test methods used are typically structured, manual test scenarios that are designed to provide specific evidence of the presence and effectiveness of each security feature. For example, the testing to verify correct operation of the SSL version 3 encryption would consist of a combination of test techniques. First, the configuration of the Web Server would be verified by human review to ensure it was set to accept only SSL version 3 connections with 128-bit encryption. Second, the data stream on a typical connection would be captured and analyzed to verify that encryption was occurring on all data.

The penetration testing activities are conducted as a separate activity once the system is in a secured production-ready state and repeated periodically throughout the system life cycle. This testing is loosely structured, so as to maximize the opportunity to discover unanticipated security vulnerabilities. The test methods include a combination of automated vulnerability test tools and manual analysis and exploitation techniques. Hostile test techniques are used to evaluate whether the system is vulnerable to those simulated attacks. As with compliance testing, the goal is to collect evidence of the effectiveness of security features. However, this testing would go further by seeking ways to bypass or defeat controls by presenting the system with hostile and/or bogus data.

The two types of testing are complementary and together provide a very thorough picture of the security posture of the system and a good body of assurance evidence that can be reviewed by state certification authorities as part of their acceptance/accreditation decision.

The ITA also segregated its testing activities into infrastructure and application steps. The infrastructure step included all security testing of the physical hosting facility, personnel security measures, security policies and procedures, and the technical features of the supporting IT infrastructure: communications networks, server operating systems, database management system, and other supporting utility software. The application step included all security testing of features of the SERVE system application software, specifically the user interfaces and the business logic that controlled the interaction between different SERVE system user classes and the data stored and processed by SERVE system. This was a convenient separation because the two areas were ready for testing on different schedules and also required different test techniques.

6. Evaluation of the SERVE Project

Evaluating how Internet registration and voting impacts the success of the voting process for UOCAVA citizens was a key goal of the SERVE project to respond to the Congressional mandate for a report on the project's effectiveness. The evaluation process had multiple components that would have determined how SERVE affected the following groups:

- The UOCAVA citizens who would register and vote using SERVE;
- local election officials (LEOs) who would manage and use the system;
- voting assistance officers, who inform military and overseas civilians about the electoral process; and
- interest groups who also assist potential voters.

These groups all play important roles in the implementation of any Internet registration and voting system that will serve the UOCAVA population. By having a comprehensive evaluation plan, it would be possible to provide a realistic evaluation of the strengths and weaknesses of the SERVE system and Internet voting more broadly.

6.1 Goals of SERVE Evaluation Project

The goal of SERVE was to examine whether Internet voting is effective, affordable, accessible, and secure. The primary goal of the SERVE evaluation project was to design and implement a scientifically based evaluation that could determine whether this overall goal was met. To accomplish this, two important questions were identified that the SERVE evaluation project needed to address.

1. Is remote Internet registration and voting an effective, affordable and secure method to improve absentee uniformed services and overseas citizens' access to the polls?

2. What do we need to know to implement this type of system as an alternative to the traditional by-mail process?

These two questions serve to frame the evaluation methodology.

6.2 Evaluation Design

The SERVE evaluation design built upon a commonly used research technique, referred to as a "nonrandomized control group design with pretest and posttest." Although the name sounds confusing, it is actually quite descriptive. The design was built around four principles. First, the evaluation methodology recognized that people and organizations will self-select into the study and participation is therefore not randomized. FVAP cannot require states, LEOs, or voters to participate, the evaluation methodology was designed to control for self-selectivity. Second, data would have been collected on all key actors participating in SERVE—voters, LEOs, intermediaries, etc.—before they start their participation and then again after the election. Third, pre- and post-SERVE data would also have been collected on a set of "control groups," which would include voters and LEOs who use the traditional by-mail process. Fourth, the pre-test and post-test data for the control and SERVE participating groups would have been compared in order to ascertain the impact of SERVE program participation on the experimental subjects.

This research design is one of the most common research designs employed by social scientists and would have helped to assure that the analysis of the SERVE project was not biased by various factors, such as participant self-selection. The logic of the evaluation methodology design would have considered changes observed in post-test data, for participating subjects but not control subjects, as support for the hypothesis that the use of the SERVE system caused the changes for participating subjects relative to control subjects. By collecting a large array of data about control and participating subjects, the evaluation methodology planned to attempt statistical controls for potential confounding effects, as well as to study potential self-selection biases and to attempt to mitigate those biases.

Additionally, LEO case studies were planned to analyze the workflow of control LEOs as well as pre- and post-test for participating LEOs. This was to evaluate any modification of practice that the SERVE system caused.

6.3 Data Collection for the SERVE Evaluation

In order to answer the research questions noted above, the SERVE evaluation project required collection of a variety of different types of data. The data would have provided the information necessary to answer the basic research questions about the efficacy of the SERVE project and voting system. Additionally, it would have given a detailed understanding of the respective populations of UOCAVA voters, local election officials, and other entities involved in UOCAVA voting (especially Voting Assistance Officers and interest groups that assist overseas voters). Specifically, data that would have been collected:

- system and audit logs, which would have provided large quantities of data about system use and technical or security problems that were encountered;
- help desk logs, which would have provided information about the type of problems users encountered, attempts at resolution, speed of resolution, and any subsequent contact made regarding the original problem;
- election administration data from states and counties, which would include, for example, information on the number of voters using the UOCAVA process in 2000, 2002, and 2004, and the resolution of those ballots;
- survey data from VAOs and the private groups and organizations involved in UOCAVA voting, which would inform us about the breadth of work done by these entities to serve the UOCAVA population; and
- surveys of UOCAVA citizens and SERVE participants, which would be critical to understanding the experience of both SERVE and by-mail UOCAVA voters.
- Data from parallel test experiments and security analyses.

To the greatest extent possible, the UOCAVA voter surveys would have tracked existing questions used in other surveys of the American domestic electorate that will be available for public research after the 2004 election, like the National Election Studies and other major surveys. This will allow for better comparability of results from the UOCAVA surveys to the

American electorate, which can answer many questions about basic differences in the populations as well as other questions about technology use and political participation.

These quantitative data collection efforts were also to have been augmented with qualitative evaluations. These qualitative evaluations would primarily have involved conducting focus groups and interviews with small and specific samples of SERVE participants, including LEOs, voters, and representatives of the interest groups that attempt to reach these voters. Focus groups were to be used to develop a better context for appreciating the issues facing these various groups of voters. For example, people in the Air Force may have an easier time voting than other service personnel because they are more likely to be stationed at bases with physical military addresses. Naval personnel, by contrast, are more likely to be isolated physically onboard ships. Additionally, factors such as access to mail and Internet services, attitudes of commanding officers, and similar factors may influence the likelihood that a military person will or will not vote. These factors are hard to investigate through traditional survey methods but can be addressed through focus groups.

The quantitative survey data would also have been used to identify specific LEOs through purposeful sampling on which to conduct case studies. The rationale behind doing these case studies is to select specific, information-rich cases that provide the greatest amount of data possible for the evaluation. For example, the evaluation team considered conducting case studies on typical LEOs who implemented SERVE or unusual LEOs that had either great difficulty or great ease in implementing SERVE. Through these case studies, it would have been possible to document issues such as (1) how SERVE changes the operations and processes used to serve the absentee voting population, (2) problems that arose during the implementation of SERVE, (3) the level of service the LEOs received from the contractors in the project, and (4) other issues that the LEOs identify. Short case studies would also be conducted on UOCAVA voters through interviews, designed to illustrate issues faced by "typical" types of UOCAVA voters. For example, short case studies would have compared the typical SERVE voter, the typical voter who used the traditional absentee voting process, and the typical UOCAVA non-voter (as identified through survey research).

6.4 Key Issues Identified by the Evaluation As Implemented

Before the SERVE project was terminated, the evaluation of the project was underway. But there were several issues that would make it difficult to conduct a comprehensive evaluation of Internet registration and voting for UOCAVA voters and possibly difficulties with the implementation of SERVE. These problems included:

1. Lack of Reliable Data on UOCAVA Voting: During the LEO baseline data collection efforts, it became evident that reliable data on UOCAVA voting for the 2000 or 2002 elections was not readily available. UOCAVA voting is a form of absentee voting, and many jurisdictions had not distinguished between these two forms of absentee voting previously. Many were also unable to provide data on residual votes—ballots that were not counted or contained over- or under-votes for UOCAVA voters.

2. Low Response Rates from LEOs: Many LEOs participating in SERVE were not able to provide UOCAVA data from previous elections.

3. Low Response Rates from Intermediaries: Few intermediary groups responded to requests for information regarding their activities assisting UOCAVA voters to participate in the electoral process.

The unavailability of this important pre-test data would have made it difficult for the evaluation team to document how the experimental treatment (here the use of the Internet-based registration and voting system) might have influenced election officials or voters as they participated in the 2004 elections using the SERVE system. The unavailability of this important pre-test data also led the evaluation team to raise concerns about how much important post-test data they might have obtained, and what the quality of that data might have been. Thus, the evaluation team was considering methodologies to improve data collection during the November 2004 elections, and ways to deal with missing or low quality data had that been the status of post-treatment evaluation data, at the time the SERVE project was halted.

Section 7: SERVE Implementation Issues

There is little question that it is technically feasible to build an Internet registration and voting system. Such systems have been used in several public United States elections in Alaska, Arizona and Michigan. These systems have also been used in public elections in numerous other countries, and in countless private elections. However, many of these trials have pointed to a larger issue associated with Internet registration and voting: how can these systems be effectively implemented? There are several factors that influence the implementation of these systems, and each is discussed below.

7.1: The Election Context

Elections are not all created equal. They vary in the level of participation they attract, the type of voter who participates, the complexity of their rules and ballot designs, and the level of attention they receive. As efforts are made to implement Internet registration and voting solutions for UOCAVA voters and others, it is important that this context is taken into consideration. Specifically,

- Getting states and counties to participate.
- Recruiting voters.
- Credentialing voters.
- Accommodating varied state election laws and practices in a single system.
- Local election officials differ in the level of technological sophistication they exhibit in the election administration and voting technologies they use, and the staffing capacities they have.
- Elections differ in their perceived importance, in the level of competitiveness among candidates, and in the typical turnout that accompany them. SERVE was being developed for an election that was perceived as highly important (a presidential election), that is closely contested, and which there is considerable interest. Additionally, some of the states where SERVE was to have been deployed are considered “battleground” states; places were the potential existed that a small number of ballots might have influenced the election outcome.
- Elections also differ in the rules that govern them. For example, primary elections often have complicated rules governing participation and ballot design. In many states, primary elections are actually private elections run by the political parties; developing an Internet voting system that can incorporate these party-based rules that vary across states can be complicated.

- Even in general elections, states have differing rules that govern elections and any system has to be able to address these differences. These rules should be identified at outset of any system deployment through a development process that includes a wide array of potential stakeholders.

- Last, some elections receive a high degree of external scrutiny because of past problems; given the many problems observed in the closely contested 2000 presidential election, there is very close scrutiny of election administration practices and voting technology in the 2004 election. Thus, elections differ in the level of external scrutiny they generate.

7.2: Participation

Participation in the development and implementation of Internet registration and voting should be viewed broadly because, in the case of UOCAVA voters, so many different entities must be involved in a successful implementation. The obvious center of any participation effort is the states and LEOs deploying the system. They have to agree with the goals for the project, and be satisfied that the system will serve the needs of their UOCAVA voters and link with their existing systems and procedures. The states and LEOs, in turn, determine the number and type of UOCAVA voters who can participate in an Internet voting project.

Participation in a project such as SERVE requires a strong commitment by both the state and the LEO, especially since UOCAVA registration and voting is a very small component of the overall election administration process facing LEOs. In order to participate, LEOs need to be convinced that the cost of their participation in the project is low, and the potential benefits outweigh the costs. Because states and LEOs were making this calculation with SERVE, it was often difficult to get potential participants to make a strong commitment. Several deadlines that had been set for finalizing participation in SERVE were pushed back in order to accommodate the needs and desires of states and localities. In some cases, states needed to pass special legislation in order to participate in SERVE, since ballots were been transmitted electronically, not by paper. Other states and localities wanted to see what the final system design would look like before finally committing to participate in the project.

Getting the cost-benefit equation to work means that integration of future demonstration projects with existing election administration practices must be as simple and streamlined as possible; it also means that future projects ought to start by documenting the requirements of a voting system for local election officials prior to the initiation of system development. Given the very different capacities that LEOs bring to an experiment like SERVE, it might have been beneficial to establish some baseline standards to participate, beyond the requirement that they have a threshold number of UOCAVA voters. A minimum requirement would have ensured that the participating LEOs were best able to utilize the technology, although this would have also reduced our understanding about the universal application of Internet voting across LEOs.

The threshold number of UOCAVA voters can also affect the way in which a system like SERVE must be integrated with a LEOs existing election administration software. In SERVE, there would have been fully integrated counties, where system applications would have seamlessly integrated with these existing systems, and other LEOs, where many system functionalities would have been accomplished manually, on a parallel system. There is a point when the manual process becomes too costly for a LEO to implement and complete software integration is necessary.

In addition to the role that states and LEOs play, there are many other entities that also have to support the system for it to be successful. These include the political parties, the military, major overseas civilian organizations, large multi-national corporations, other federal agencies (especially those with a large overseas presence and those that play a role in the electoral process), domestic groups—especially colleges and universities with a large overseas presence, Congress, other interest groups, and the mass media.

These many other entities may not themselves conduct elections but they play an invaluable role in educating potential UOCAVA voters about their voting rights and recruiting voters to participate in an Internet voting effort. These other stakeholders are also in a position to educate non-UOCAVA communities about the importance of future projects and to provide details about how these future projects work. In addition, they might be in a position to assist with the development and deployment of the new technologies, for example, by helping to provide voters with the digital signature credentials that may be needed for an Internet voting system. Having their support for any system is critical for obtaining their support and assistance in making any deployment a success. Many of these groups also bring expertise to the voting experience that could be of benefit to system developers and should be exploited as a system is being designed.

7.3: Credentialing Voters

In most American states, a voter must register before they can cast a ballot, so that the LEO knows which voters should receive an absentee ballot, and which ballot style the voter should receive. UOCAVA voters who wanted to vote over the Internet using the SERVE system would have followed this same process; they must register to vote and be approved by the LEO before they could receive a ballot. However, to ensure the registered voter is the same voter casting a ballot and to provide the voter the correct ballot, an Internet voting system must have some identification and authentication process (I&A). This I&A process might be conducted with digital certificates or other identification process similar to that used daily by individuals conducting electronic transactions at their ATM or online.

Fortunately, one part of the UOCAVA population—uniformed services and Department of Defense personnel—has digital credentials provided to them by the federal government. Many other federal employees overseas, such as embassy personnel, as well as private sector companies, also have digital identification. Unfortunately, the digital certificate technologies that are used across federal agencies and the private sector companies are not fully compatible. An effective Internet voting system for UOCAVA voters must have the capacity to support varying credentials so that the maximum number of federal personnel can participate in the easiest manner possible.

In the SERVE project, a difficult issue was the process of getting identification credentials to civilian individuals who do not have them. In SERVE, this process was to have been facilitated by “trusted agents”—specifically, overseas groups and government entities—who could officially vouch for the identity of a given civilian just as a notary does for legal purposes. The SERVE digital identity would have been good only for participation in the SERVE project, and given that SERVE was intended to be an experiment, this was fully appropriate. However, because the trusted agent process required an individual to meet face to face with a trusted agent, it is quite possible that logistical problems would have arisen at the point. Two problems would have been that individuals who were to serve as trusted agents would have to be vetted, and then interested UOCAVA citizens would have to find these trusted agents in order to be vetted themselves. This process might have hampered UOCAVA citizen participation.

Given that the federal government, other governments, and the private sector are all encouraging the public to use electronic means for transactions with the government, it may make sense to develop standard criteria for recognizing and sanctioning digital certificates that meet minimum established standards. As of February 2005, the federal government has such a standard for federal employees and contractors: Federal Information Processing Standard (FIPS) 201, Personal Identity Verification for Federal Employees and Contractors. All federal agencies are developing plans to implement FIPS 201. Until FIPS 201 is implemented, government agencies and private sector companies can certify their digital certificate process with the Federal Bridge Certification Authority (FBCA). By having standard criteria for digital certificates that are recognized for voting and other government transactions, individuals could procure such a digital certificate with the knowledge that it would be useful for an array of activities, including e-government.

A recent study of electronic signatures conducted by the IBM Center for the Business of Government found that the Internal Revenue Service e-file program has developed a means of using a personal identification number (PIN) electronic signature system. This allows taxpayers to file their tax return electronically, without having to also file a signed paper tax return as well. Because the PIN is based on personal information known only to the tax filer and the IRS, the system is easy for the tax filer and both cost effective and secure for the IRS. As the executive summary of the report notes,

> “the IRS's use of PINs and shared secrets to sign electronic government transactions on a relatively large scale demonstrates that public organizations may be able to address what is generally reported to be a major problem facing e-government. …Given the perennial public and congressional scrutiny of the IRS, it stands to reason that other government organizations should be able to utilize some of these techniques to eliminate paper signatures in e-government programs—with taxpayers’ confidence and stakeholders’ acceptance.[18]

The IRS has the advantage of having an ongoing relationship with its customers, as well as having access to information about their clients that can be used to develop a pool of potential shared secrets. Although there is less of an ongoing relationship between LEOs and voters, people who have previously registered to vote do have shared secrets with their LEO, albeit less

[18] Steven H. Holden. 2004. *Understanding Electronic Signatures: The Key to E-Government.* Washington, D.C.: IBM Center for The Business of Government.

than an individual does with the IRS. However, it would be possible to remedy this in the future by asking for certain additional information in the voter registration process.

7.4: Publicizing the program and recruiting participants

The SERVE project was ambitious as it sought to involve as many as 100,000 UOCAVA citizens from more than 50 participating jurisdictions. The recruitment of program participants loomed large as a significant task, as the program needed to reach out to get state and local election officials to participate, to obtain the active participation of individuals as “trusted agents”, and most importantly to recruit individual UOCAVA citizens from specific counties to register and vote using the SERVE system.

Recruitment of participants—especially “trusted agents” and potential voters—was clearly going to be a difficult logistical task. UOCAVA citizens, and individuals who could serve as “trusted agents”, are spread in locations throughout the world. There is not a single and simple method that can be used to communicate with UOCAVA citizens, in particular, those who are not members of the Armed Forces. Getting the word out about the SERVE project to potential voters was to be the goal of an extensive outreach effort, involving the use of various strategies to communicate with UOCAVA citizens.

The planned communication strategy would first have involved established organizations (both governmental and private), which have a myriad of methods for communicating with their members. For example, a multi-national corporation can communicate with potential UOCAVA voters through company newsletters, emails, and office signage. Other organizations are potentially even better equipped to educate potential UOCAVA voters. For example, the Department of Defense, the Peace Corps, the Department of State, and “Semester Abroad” programs are all in a position to incorporate voter education and voter credentialing into their existing protocols that are followed before an individual goes abroad. However, such efforts require planning and close coordination between the project implementers and these other organizations.

Second, a serious and coordinated media campaign would also have been necessary to educate overseas civilians about the availability of this new voting system. Through a combination of media strategies, employing both free and paid media outlets, information about the availability of a new voting system and how it can be utilized would be widely disseminated throughout the overseas communities. Part of this media campaign could build upon the internal communication efforts that are a part of any large organization. For example, the Department of Defense has built in mechanisms for communicating with its members, just as a multi-national corporation would. Leveraging these communications networks within organizations is critical to successfully reaching potential UOCAVA voters.

Last, the outreach efforts to involve UOCAVA citizens in this new voting system trial needed to include state and local election officials. Their active participation in voting system experiments is obviously critical, as they are also an important resource of information for overseas citizens about the election process. Involving the LEOs in publicity is critical, and could range from simple efforts like assisting all participating LEOs develop a variety of outreach programs so they can attempt both passive and active attempts to contact UOCAVA citizens from their jurisdictions to inform them about the new voting system, to broader efforts to assist state and local officials with outreach to media outlets and intermediary organizations in their geographic vicinity.

7.5: Integration with local systems

Over the past decade, many LEOs have made substantial investments in new voting technologies (from new voter registration systems to new precinct voting equipment) and such investments are likely to continue as LEOs move away from punch cards and paper ballots towards electronic technologies. These transitions have been facilitated in recent years by HAVA, and HAVA-mandated changes will continue to lead state and local election officials throughout the nation to acquire and use new technologies for election administration in coming years. These investments have primarily been with proprietary systems that are designed to provide a LEO with end-to-end services for all election administration procedures. One downside of these systems is that they are not designed to integrate with auxiliary systems, such Internet voting technologies. What they lack are a common standards-based software interface, common data exchange functionalities, and the ability to link varying voting systems.

System integration in the SERVE project was further complicated by the simple fact that most election administration systems are heavily oriented towards in-person precinct voting activities. In the past, much of the election administration process involved the logistics of supporting in-person precinct voting. Absentee voting, especially voting-by-mail, has not been a major component of election administration outside a few states like Oregon, Washington and California. Furthermore, the specific tasks associated with UOCAVA absentee voting are even one step further removed from the main focus of election administration activities, meaning that integration must take into consideration the sometimes low-tech and jurisdiction-specific methods that are currently used to manage UOCAVA and other absentee voting activities.

Future deployments of Internet registration and voting will need to address these problems, as systems integration is likely to become an increasingly difficult problem to resolve as election administration is becoming a more and more technological process. There are several models by which this can occur. Most effective and most promising would be for voting system vendors to adopt a common protocol for data exchange and software interfacing. This would allow, for example, a LEO to create ballot definitions using one system and then export those definitions to the Internet voting system. Likewise, ballot tabulation processes and procedures would be integrated as well, facilitating the easy reporting of results. This protocol could come from either the federal government, through requirements from the Election Assistance Commission, from other standard setting bodies, or from the efforts of the system vendors themselves.

As part of the SERVE development process, multiple integration tools were developed so that all elections data from various voting systems could be translated into a standard file to integrate with the system. This standard protocol would allow the system to link with any electronic voting system and election management system. With a common protocol, a LEO could fully automate the process of preparing an Internet registration and voting system for usage. However, not all jurisdictions may want, or have the capacity to, operate such a fully automated system. In this case, it may be more logical for LEOs to utilize a service bureau to provide many of the operational functionalities for Internet voting, especially the entering of ballot definition data. In essence, the service bureau acts as the printer, providing LEOs with completed ballots based on the raw data provided by the LEO. This process allows less technologically sophisticated LEOs or those with fewer personnel resources to still participate.

Some other recent trends, however, may make it easier in coming years to develop and deploy Internet-based registration and voting systems for UOCAVA citizens, in particular the on-going development of statewide voter registration systems. These systems will better standardize the voter registration process—and database—within states, meaning that some of the integration tasks might be easier to accomplish in the near future as states deploy statewide voter registration systems. In some states some of the election administration process is shifting to a more uniform statewide system (for example, the state of Georgia), and these broader trends towards statewide uniformity may also make system integration a less complicated task than it was with the development of the SERVE system.

7.6: End-User Support

Because Internet registration and voting is a new activity, it is critical for all parties involved in the process receive a complete compliment of end-user support services. These include deployment and integration support, LEO training, voter education materials, and help desk support for both LEOs and voters.

The end-user support begins with deployment and integration services. The SERVE team worked with LEOs to determine how the system would work within their existing election administration system and assisted in integrating these two systems together. They also met extensively with LEOs to plan the timing of the system deployment.

Once the system deployment was ongoing, LEO staff would be trained to use the system. Because UOCAVA registration and voting is not a primary task in most election offices, any training for a new UOCAVA voting system must be done effectively and with a minimum of disruption to the primary activities of election staff. This training will involve a variety of players, from system vendors, to state and local LEOs who will operate the system, to intermediaries who may have to sign up individuals for digital certificates. As a general rule, the need for training with the system should be minimal; a well-designed system should be intuitive and designed to walk a user through its operations. However, there will be individuals who want training and will benefit from it, and the key is to design a training process that will stay with a user after the training is complete. The smaller number of UOCAVA voters and the newness of a system like the system create challenges for training LEO staff.

Development of a usable and effective program for training all of those involved in the deployment of the voting system is critical for the success of future trials and experiments with new voting technologies for UOCAVA citizens.

Finally, any future system will also need to have similar voter education and help desk support as was planned for SERVE. The SERVE system would have provided extensive help desk support services for both LEOs and voters who encountered difficulties, including both telephone and email support. Such a system is again needed because of the newness of an Internet voting system for UOCAVA voters and the geographic diffusion of these voters.

7.7: Standards for Certification

As the SERVE system was being developed, there were no voting system standards available for Internet registration and voting systems. No federal entity (e.g., Federal Election Commission, the Election Assistance Commission) or private entity (e.g., IEEE) has promulgated standards for certifying an Internet registration and voting system. There are, however, standards for certifying electronic voting systems, and these standards can be used to identify key requirements for an Internet voting system, which is largely a remote electronic voting system.

In SERVE development, three key actors were involved in system certification—the FVAP, an ITA making recommendations regarding system certification, and the system designers—reviewed all relevant voting system standards and identified all of those that applied to an Internet voting system. The existing Voting Systems Standards (VSS) provided the basis for conducting the certification evaluation for SERVE. However, as is addressed in another section of this report, as the existing VSS does not address Internet voting systems, the protocol developed for certification of the SERVE system was somewhat ad hoc.

The scheduling of certification activities required coordination across the entire project. Development and certification need to go together hand-in-hand, so that questions about the correctness of the system design and build can be addressed as close to real time as possible. In the traditional system certification process, system designers have a reference to work with in the development process; with Internet voting, system developers need close guidance to address the issues that arise. There is also recognition that the current certification process is not transparent for developers, who often need critical information from the ITA.

One key issue that arose in SERVE is that the existing VSS does not have many testing and certification procedures for the security of voting systems, especially Internet-based voting systems. The VSS also does not address voter registration systems.

Significant security precautions were built into the SERVE system. Also the SERVE system was developed with and would involve a voter registration process that was highly automated and largely electronic, a process to test and certify the system security and voter registration software was developed. The details of this process are provided in other sections of this report, but the lack of security standards and standards for the testing and certification of electronic voter registration software is an area that needs future research and resolution.

These standards should encompass not just the system software, but also the system’s accessibility, usability, and hosting arrangements. The standards should also contain an end-to-end review, running from the authentication and registration of voters in the system, to ballot definitions and design, to balloting, tabulation, and provisions for auditing and recounting. Voting system standards typically cover just that—the entire voting system. In the case of Internet registration and voting, there are other critical features to evaluate, including voter registration, ballot design, and vote tabulation. All of these features must be included in any voting system standards for future Internet registration and voting systems.

In a related manner, there also needs to be a clear process for how an Independent Testing Authority (ITA) is involved in the certification process. Typically, ITAs are hired by and paid by the system vendor and developer to test and certify the voting system. This arrangement is not uncommon in regulatory settings; having the regulated party pay for the evaluation keeps the public from footing the bill for a process that will ultimately profit the regulated party. However, the existing process results in less transparency than might be warranted in the case of voting systems and does have obvious incentive problems. Therefore, having the ITA work for and by hired by a federal or state entity—for example, the Federal Voting Assistance Program or the Election Assistance Commission—but paid for by the system developer, would provide for a layer of independence in the process and ensure that it was the state, and not the system creator, that was ultimately hiring the ITA and was being informed about the status of the system certification. More critical examination of the ITA process for future development and deployment of Internet registration and voting systems is necessary.

A final issue with the certification of an Internet voting system is the question of configuration management of the deployed system. The configuration management of the certified, controlled software requires the intervention of a third party that can escrow the original software and then rapidly determine whether any proposed patches or changes do or do not affect the functionality of the system software.

7.8: Risk Analysis and Mitigation

All technologies have inherent risks associated with them, both real and perceived. Electronic voting, including Internet registration and voting, is no different and there are risks associated with this registration and voting method. What is critical, however, is for these risks to be evaluated quantitatively and in the right context. The traditionally identified risks associated with Internet registration and voting have corresponding risks in the paper-based voting realm. For example, an Internet denial of service attack that would prevent a voter from accessing an online voting engine is similar to the problems a voter faces using the by-mail system. In both cases, the voter cannot effectively access their ballot. One difference, of course, is that once a voter cast their vote by-mail, they are at the mercy of the mail. In an electronic denial of service attack, a voter might be able to go back and attempt to vote later, since balloting is instantaneous once completed. Another difference is that an attacker might be able to mount a denial of service assault on an Internet voting system that is larger in scope than might be possible to mount for the by-mail process.

8: Recommendations for Future Demonstration Projects

As this report has shown, much was learned during the SERVE project's development phase. In this section, we provide recommendations for future projects like SERVE. To summarize, the major recommendations from this report are:

1. Work up to a large scale system.
2. Recognize the variations in state and local laws and procedures.
3. Build consensus of key stakeholders.
4. Identify and address risks.
5. Improve development and testing processes.
6. Standardized interfaces for voting systems.
7. New models for standards, testing and certification, especially for Internet-based registration and voting systems.
8. Improved data collection on UOCAVA citizens.
9. Project Management.
10. Assess methods for electronic voter authentication.
11. Monitor other Internet voting experiments.
12. Provide funding for future development and research of improved ways to help UOCAVA citizens register and vote.

Below we discuss each recommendation in more detail.

8.1 Work up to a large scale system.

One conclusion is that the SERVE project was quite ambitious. It involved the development of a novel and unprecedented Internet-based registration and voting system; to be developed, tested, certified, and implemented in a relatively short period of time; involving the participation of seven states and over fifty counties; aiming to include the active participation of perhaps as many as 100,000 UOCAVA citizens from around the world; all to be done in a closely contested presidential election season and an environment in which election procedures and voting technologies were being closely scrutinized.

In future projects, the scope and nature of the project might be much more limited, especially in initial phases of the project. Typically, in the world of election administration, the roll-out of a new voting system takes a series of election cycles to complete: extensive training of election workers in the use of the new voting system is necessary before the first use; in many if not all new voting system implementations there is active assistance from the system vendor the first few elections the new system is used; and there is post-election analysis of problems that arose, re-training, and in some cases re-development of the voting system.

Thus, future projects like SERVE should probably start small, both in terms of the number of participating jurisdictions and in the types of elections the system is initially used in; perhaps an initial implementation in a small number of states, in a non-presidential election, would be ideal. Primary elections should be avoided until after several iterations of the system have been deployed. States have very different rules for primaries versus general elections. Then, building on the lessons learned in the first trial, the voting system could then be used in more jurisdictions, perhaps in a federal but non-presidential election. Again, building on lessons learned, the voting system could then be prepared to be used in an eventual presidential election, in a much broader set of states.

This would require a project that spans a number of election cycles, and a process by which system development would be on-going, reflecting the lessons learned from each use and evaluation of the voting technology. An incremental development, implementation, and evaluation path should be articulated at the initiation of future projects. Key measurable milestone goals should be specified for each stage of future projects, especially focused on quantitative documentation of how the project is resolving known UOCAVA registration and voting problems.

8.2 Recognize the variation in state and local laws and procedures.

Election administration in the United States is typically a matter of state and local law, as well as customs and cultures of localities throughout the nation. While the federal government does regulate federal elections, and is active in overseeing goals like equal protection and the preservation of basic voting rights, in general the federal government has largely delegated to state and county governments much discretion when it comes to election administration.

This has resulted in an election process that is can seem complex; basic issues (but ones important for the development of voting systems like SERVE) like how ballots are designed or what information is contained in post-election tallies of election results vary greatly over the nation. This complexity makes it difficult to develop a centralized registration and voting system like SERVE. This complexity also means that future systems should be developed with this variability and complexity in mind.

There are two ways in which a voting system like the SERVE system can be designed: (1) through the design of system architecture and the imposition of that architecture across jurisdictions, or (2) by design of an architecture based on basic first principles that have been enunciated by local jurisdictions as critical components of a voting solution for their needs. This latter design and development process is one that requires working closely with local election officials in order to fully understand how they administer elections, to determine the mission critical features of election administration in participating each jurisdiction, and to also figure out places in the system design where flexibility can be sacrificed for uniformity and simplicity.

It is true, however, that HAVA is sparking some movement in states towards greater uniformity in election administration procedures and voting technologies. With the development of statewide voter registration databases, and in some places the deployment of uniform voting systems, some of this variability may be less problematic for future demonstration projects. No matter how election administration evolves in coming years, there still will be sufficient heterogeneity across states and counties to necessitate detailed analysis of local election practices early in the development of future voting systems like the system.

8.3 Build consensus of key stakeholders.

In the United States, there are many constituents for voting technologies: the voters themselves, groups that work to assist citizens register and participate, the county and state officials who purchase and use the technologies, the research communities who study election technologies, and of course the election technology industry itself. Others interested in voting technologies are members of the media and those holding—or interested in holding—political office.

The SERVE development effort worked selectively with representatives of each state interested in participating in the project, and with a small set of representatives of participating counties; these representatives constituted the SERVE "Design Advisory Group." This group was constituted after many key decisions regarding the SERVE project and design were made, and there were neither time nor resources to work to develop consensus from a broader set of key stakeholders for a project like SERVE.

Future projects should consider a different structure. As elections in the United States are a state and local affair, future projects should work to obtain consensus and buy-in from election officials in participating jurisdictions before key project and design decisions are made. The state and local officials will be the ones on the front lines during the implementation of future projects, they will need to devote time, energy, and resources to their jurisdiction's participation, and thus making sure that they are in agreement with the project's scope and direction is an important ingredient to a successful project. Also, future demonstration projects might consider different arrangements to produce a stronger state and local investment in the project; for example, by allowing participation only from jurisdictions that promise to dedicate a certain level of resources (for example, staffing) for the development, implementation and evaluation of those future voting systems. States and counties must commit to participate long before system design is scheduled to be complete.

Furthermore, future projects should consider seeking the input of representatives from the broader constituencies of voting technologies. The fact that the SERVE project was predicated on the experimental nature of the project, and that it contained a deliberate and pre-meditated evaluation effort, is an important step in this direction. Few other voting system development and implementation projects have had pre-meditated evaluation components, nor have provided post-project analyses that are scientific in nature.

But in addition to building in an evaluation component, future projects may want to seek input from stakeholders outside the election technology business. Any change to the existing election structure is inherently political, and it is important to recognize this as efforts are made to build support for future Internet voting projects that would enfranchise UOCAVA voters. Thus other important stakeholders should be involved in future demonstration projects, ranging from other federal government organizations, to groups involved with Americans abroad, and the many groups now interested in the election process and voting technologies.

8.4 Identify and address risks.

There should be a formal process at the beginning of any future demonstration project to identify the risks associated with the system, the likelihood of these risks, and address ways in which these risks can be mitigated. This process should be open and involve participants from across the array of views on Internet voting. Because risk analysis is not only about identifying and mitigating against actual risks but also about identifying perceived risks, there should also be a concomitant public relations effort designed to educate the public, the media, and key stakeholders about the system, its purpose, and the comparative costs and benefits of the system. This public relations effort will serve to allow the broader public to understand how the system functions, the program's goals, and to educate people about the actual risks of the system, as opposed to perceived risks and to understand all risks in the correct context.

As a part of the risk analysis, the project must evaluate all commercial operating systems, to determine which will not only meet the requirements, but will also support the largest number of voters.

8.5 Improve development and testing processes

The development organization must meet a minimum of level three on the Carnegie-Mellon Software Engineering Institute' Capability Maturity Model – Integrated (CMMI). The specific development team must be monitored and evaluated periodically during the development of the system to ensure compliance with the CMMI processes.

As a part of the development processes, a robust technical documentation process must be in place and rigorously enforced.

The testing organization must be available from the initiation of the project. Testing organizations provide invaluable assistance during design to ensure that the system will be testable.

8.6 Standardized interfaces for Voting systems.

One of the most challenging issues that arose during the development of the SERVE architecture was the wide variety of different voting systems that are in use even in the small number of election jurisdictions that were hoping to participate in the SERVE project. Some election jurisdictions in the United States have adopted a "unified" voting system, where they use products from a single vendor that are highly integrated. Other election jurisdictions use mixtures of products, with systems from one vendor that handle voter registration tasks, systems from other vendors that run election-day balloting, and so on. And many election jurisdictions have voting systems that have evolved over years of use, as systems have been changed or patched to solve earlier problems.

The daunting problem for development of a voting architecture like SERVE is how to insure that all of the components of the voting systems currently used by election officials can integrate effortlessly with the SERVE registration and voting system. Unfortunately, there exist no current standards that govern the interface between various components of voting systems. There are no standards that dictate that information that comes out of a voter registration system must have a certain format so that it can be directly used by an absentee balloting system, for example.

Standards for information exchange between components of voting systems need to be developed, so that voting architectures like SERVE can be developed in the future. These standards are also critical for the continued development of current and future generation voting systems, so that election officials will have an easier time selecting voting system components for their particular needs; by having standardized information exchange practices, election officials can more readily view the acquisition and use of new voting system components as "plug and play." Furthermore, standardization of information exchange across voting system components will regularize the information flow, and mean that there will be consistent and auditable information that moves through a voting system.

8.7 New models for standards, testing and certification, especially for Internet-based registration and voting systems.

Currently there exist no standards for Internet-based registration and voting systems. The most recent round of federal voting systems standards (VSS) enacted in 2002 expressly did not provide standards for Internet-based voting systems. However, for future voting systems projects like SERVE to be successful, standards, testing, and certification procedures for Internet-based voting systems should be developed, so that the future projects have clear guidelines for what the basic parameters for the use of these voting systems will be.

The 2002 VSS did not provide standards for electronic voter registration systems, nor for how those systems interface with voting systems. As election officials increasingly move to highly automated and electronic voter registration systems, the practice of election administration is evolving to one where much of the voter registration task will be software-based. This is increasingly the case as states move to implement the HAVA statewide voter registration database requirements. Given the replacement of human actions with software, it becomes imperative that standards, testing and certification of voter registration systems and their interface with voting systems be produced.

In the absence of new voting systems standards that cover Internet-based registration and voting systems, future demonstration projects should carefully consider how they will integrate certification and testing into project development. Key recommendations for future demonstration projects in this regard are, first, that a testing and certification team be identified immediately upon initiation of the project so that they can be involved from the initial stages of project development. Second, the certification and testing process should exist in parallel with development efforts; this will help insure that the certification and testing process evolves appropriately as the system is being developed, and will help make system development more effective. Third, specific interpretations of the standards being utilized during the future project's testing and certification need to be documented and retained, so that those interpretations can form the framework for the actual development of actual future voting systems standards for these novel registration and voting systems.

8.8 Improved data collection on UOCAVA citizens.

In order to understand how to build voting systems to improve the UOCAVA citizen voting experience, it is imperative that more data be collected on UOCAVA citizens and their voting experiences. Important efforts to collect data on the UOCAVA voting experience are currently undertaken by the FVAP as part of their evaluation of UOCAVA participation in each federal election. Much more information needs to be collected from election officials across the nation, to provide a more comprehensive analysis of the problems that are being faced by UOCAVA voters when they try to register and vote.

Each election jurisdiction in the nation should compile and make available information on the number of UOCAVA FPCAs and FWABs they receive in each federal election. Also, data on the disposition of all FCPA and FWAB applications should be retained and made available. Information regarding the fate of every UOCAVA ballot returned should also be retained and made available for research and evaluation efforts.

Having more comprehensive historical information on UOCAVA registration and voting, as well as the experiences of UOCAVA citizens as they try to register and vote, is imperative for attempts to evaluate future demonstration projects. In the vernacular of the natural sciences, an easy way to understand the impact of an experimental treatment (here the use of a newly-developed voting system) is to compare outcomes before and after the treatment has been administered. In other words, we want to see if the use of a newly developed voting system has made for a better voting experience, relative to past voting experiences. Only by having high-quality historical information is such a before-and-after analysis possible.

Last, not only is there a pressing need for the collection of comprehensive registration and voting data on UOCAVA citizens, there is also an important need for the collection and analysis of information more generally on the American population living abroad. Estimates on the American population abroad, and in what parts of the world they are located, vary widely.

8.9 Program Management

A program office must be established and appropriately staffed with the correct numbers and skills mix to establish a rigorous project information management process at the initiation of this project. There is a need to capture the process as well as the technical results.

A management board of election officials should be established to oversea the project. This would provide a political buffer for the Department of Defense, since a project of this nature is inextricably bound to the electoral process.

8.10 Assess methods for electronic voter authentication.

The SERVE system was designed to incorporate a very sophisticated voter authentication procedure involving digital certificate technologies. While an important design goal, it is unclear how this voter authentication technology might have worked in practice:

- We do not know how many potential participants would have had access to CAC technologies and how familiar they are with their use.
- We do not know how well the "trusted agent" approach might have worked in practice
- It is unclear how usable the digital certificate process would have been for voters (most of whom would have had little experience with this technology).

In the end, it is not clear this sophisticated technology was necessarily required for voter authentication, or whether other technologies might be better suited to the task.

In future projects, how voters are authenticated to use the system will be an important design decision, and not one to be made quickly. Five important questions must be answered: how high is the required level of security for voter authentication, what are the options available for voter authentication, how usable is each authentication system, how secure is each authentication method, and how far must accessibility be sacrificed for the sake of system security? We consider these issues open topics for research in future demonstration projects.

It is not necessarily clear that digital certificate technologies are optimal for electronic voting systems, nor that they are even necessarily required. After all, the Internal Revenue Service (IRS) has recently avoided the use of digital signature technologies for their electronic tax return filing system, instead using easier authentication schemes utilizing personal identification numbers and knowledge-based authentication. The IRS electronic tax solution, however, is predicated on the fact that the IRS has substantial information on would-be electronic tax filers, based on the previous tax returns. It is likely that many UOCAVA citizens, especially those not already equipped with some digital identification like the DoD CAC, may have previously registered to vote in some jurisdiction and had their identity verified in-person by an election official at that time. It might be possible for future demonstration projects to employ authentication solutions like that used by the IRS for UOCAVA citizens who have already completed an in-person registration process before they left the United States. Thus, future projects should consider a range of authentication procedures, determine what the required level of security is, and should fully evaluate their security and usability before making this fundamentally important design decision.

8.11 Monitor other Internet voting experiments.

The Federal Voting Assistance Program and the Election Assistance Commission should monitor other Internet voting experiments worldwide to determine what we can learn from these efforts.

8.12 Provide funding for future development and research of improved ways to help UOCAVA citizens register and vote.

The SERVE project, like the VOI project before it, was an ambitious attempt to improve the registration and voting experience for UOCAVA citizens. The SERVE system might have drastically reduced ballot transit time, reduced error rates in UOCAVA ballots, and could have made the UOCAVA process easier for participating LEOs. As we have documented in this report, even though the SERVE system was never used for live voting, a great deal was learned during the development phase of the SERVE project.

Efforts must continue to develop new and improved ways for UOCAVA citizens to register and vote. This research agenda should examine in detail the wide variety of ways that new technologies can improve the registration and voting process for UOCAVA citizens, including web-based approaches for registration and balloting (like the SERVE system), web-based and email ballot delivery, and the use of fax technologies for ballot delivery and return. While election jurisdictions throughout the nation have experimented in very limited ways with some of these other technological innovations for UOCAVA registration and voting, these efforts need to be better funded, better studied, and placed within a rational development agenda.

The future of election administration in the United States will see the continued use of new technologies. While the technologically-ambitious SERVE project was not used for live balloting in the 2004 elections, this is not necessarily a sign that new technologies will never again be considered for UOCAVA registration and voting. Instead, we need a policy strategy that examines the wide variety of possible applications of new technologies for UOCAVA registration and voting, and that fully funds the efforts to develop new registration and voting solutions for these voters—and which also fully funds efforts to evaluate their effectiveness and to document for the public the pros and cons of different technologies for UOCAVA registration and voting.

8.10 Learn from experience

The United States is not currently a leader in Internet registration and voting. Other nations are currently conducting formal and well-planned experiments with Internet voting and are moving forward using many of the principles identified above. Some other nations are examining or experimenting with electronic technologies to assist their citizens abroad to participate in their own elections. Regardless of whether the United States develops a formal research and development program to develop and implement new voting technologies for overseas citizens, the Federal Voting Assistance Program and the Election Assistance Commission should track these projects by other democratic nations in order to learn more about the success and pitfalls associated with Internet registration and voting.

In particular, there are some important questions that the experiences of other nations can provide regarding the use of electronic technologies like the Internet for registration and voting. For example, what are the documented risks associated with the use of the Internet for registration and voting, and what procedural and technical steps can best mitigate these risks? Experiments and trials in other nations can provide real data that can help better estimate threats for future demonstration projects in the United States. Second, how do these other trials and experiments effect voters --- are there noticeable effects on voter participation, accuracy of balloting, perceptions of interest in elections and their integrity? Third, how do these new technologies improve the ability of election officials to administer elections, and in what ways do these technologies potentially complicate election administration? There is much that we can learn from the experience of other nations as they experiment with using the Internet for running their elections.