Department of Defense:
Expanding the Use of Electronic Voting Technology for *UOCAVA* Citizens

As Required by Section 596 of the
National Defense Authorization Act
for Fiscal Year 2007

May 2007

Table of Contents

EXECUTIVE SUMMARY

As required by the *National Defense Authorization Act for Fiscal Year 2007*, Public Law 109-234, this report discusses plans by the Federal Voting Assistance Program (FVAP) for expanding the use of electronic voting technologies for citizens covered by the *Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)* for the 2008 presidential election and the 2010 general election. Included is a summary of previous and ongoing electronic voter assistance projects undertaken by the FVAP, electronic voting projects undertaken independently by the states and territories, and electronic voting projects developed in other countries.

The Electronic Transmission Service (ETS) is a toll free fax option started in 1990 for local election officials and all *UOCAVA* voters to send and receive (where permitted by state law) applications, blank ballots, voted ballots and other official election materials. Voters have the ability to send and receive absentee balloting materials through toll free fax numbers in 51 countries. A fax-to-email conversion capability was added in 2003.

The FVAP implemented the Voting Over the Internet (VOI) Pilot Project for the November 2000 general election. VOI examined the feasibility of using the Internet as an alternative method for secure, remote absentee registration, ballot request, and voting for all *UOCAVA* citizens in participating states. VOI provided the first opportunity for binding votes to be cast over the Internet in a general election for federal, state, and local offices. The *National Defense Authorization Act for Fiscal Year 2002*, Public Law 107-107, directed the Secretary of Defense to carry out a demonstration project that would enable absent uniformed service voters to cast ballots through an electronic voting system in the 2002 or 2004 general election. While not taken to its intended conclusion, the SERVE 2004 project yielded useful information for the design and certification of electronic registration and voting systems, and for the direction of future innovation in the absentee voting process.

IVAS 2004 was a DoD project implemented to allow eligible absentee voters who possessed DoD identifiers to request and receive their absentee ballots via the Internet. IVAS 2006 provided two tools for blank ballot request and delivery for use by states and voters with DoD identifiers. Additionally, it provided consolidated information from the 55 states and territories on electronic transmission alternatives for ballot request, blank ballot delivery and voted ballot return for all *UOCAVA* citizens.

The Election Assistance Commission (EAC) and the Government Accountability Office are conducting studies on electronic alternatives for *UOCAVA* voting. The FVAP will take their results and recommendations into consideration as it continues to develop products for 2008 and 2010.

Almost all states and territories allow some combination of fax, email, telephone and, to a limited degree, the internet, for the request and/or transmission of balloting material. The extent of usage varies widely. The states accommodate other voting tasks

electronically. These may include checking registration status, viewing blank ballots, blank and voted ballot tracking, and voted ballot casting. Electronic voting projects in other countries are varied and ongoing. Communication technologies tested and utilized include the internet, telephone, text messaging and interactive digital television.

Upon the release of EAC and National Institute of Standards and Technology (NIST) guidelines for electronic voting, the Department will pursue the development of an internet voting strategy which may mirror the functionality and security of VOI and SERVE. A complete internet voting system would provide voter identification and authentication, voter registration, election administration, ballot delivery, voting, tabulation, and results reporting. Depending on the recommendations included in the guidelines and the final design of the system, full development, testing and deployment would require an estimated 24 to 60 months.

In planning for future tools, the FVAP will consider lessons learned from the 2006 election as well as observations from the participating states, studies and reports from the EAC, technologies already in use for elections in the 55 states and territories and countries around the world. For the 2008 elections, the FVAP intends to implement ballot request and delivery tools that are flexible, convenient and as secure as possible. The tools should be delivered to the states as far in advance of the election as possible. The FVAP needs many months to involve and train the states and territories, particularly when the project involves processes that may be different from the existing state and local election official practices, as well as to reach out to *UOCAVA* citizens. The FVAP and the states will maintain the toll-free ETS and related services, and the FVAP will continue to promote its legislative initiatives, encouraging the expansion of electronic alternatives for *UOCAVA* voters.

In March 2007, the FVAP and the DoD's Business Transformation Agency released a Request for Information to solicit from industry general electronic solutions that satisfy 3 absentee voting tasks: voter registration, ballot request, and blank ballot delivery. Solutions need to support varying state requirements and legally allowed methods of transmittal.

In June 2007, the FVAP will issue Request for Proposal (RFP) to solicit specific technological solutions that satisfy the Department's electronic voting requirements. The RFP will be structured to accommodate a multi-phased development plan comprised of a base system and 2 options. The base system will provide for voter registration and ballot request for all *UOCAVA* citizens utilizing an automated FPCA embedded with state-specific requirements. The 2 options are: 1) blank ballot delivery and 2) digital signature identity management for both state officials and citizens utilizing CAC cards as well as comparable certificates issued by other approved authorities. These digital signatures may serve as the citizen's "wet" signature on the FPCA, and as an initial logon identifier. Barring delays caused by external variables, the following timeline is anticipated:

- June 2007 – Release of the RFP
- August 2007 – Responses to the RFP will be evaluated and a contract awarded

- December 2007 – Base solution availability for implementation in time for primary elections
- March 2008 – Option 1 delivery
- June 2008 – Option 2 delivery

The FVAP will engage the states early in the development process by soliciting their input as stakeholders and educating them as the final tools become available. The FVAP will use election conferences, news releases, teleconferences, letters, and other avenues to gather input from, and provide information to states, local election officials, voters, and Voting Assistance Officers worldwide.

INTRODUCTION

As required by the *National Defense Authorization Act for 2007*, Public Law 109-234, this report discusses plans by the Department of Defense's Federal Voting Assistance Program (FVAP) for expanding the use of electronic voting technologies for citizens covered by the *Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)* for the 2008 presidential election and the 2010 general election. Included as background is a brief summary of previous and ongoing projects offering electronic alternatives to the by-mail absentee voting process undertaken by the FVAP and in the states, up to and including the Integrated Voting Alternative Site (IVAS) tools used in the 2006 general election.

The FVAP's mission is to facilitate the absentee voting process for *UOCAVA* citizens living around the world. This includes consulting with state and local election officials, prescribing the Federal Post Card Application (FPCA) for absentee registration/ballot request, along with Federal Write-in Absentee Ballots (FWAB), and distributing descriptive material on state absentee registration and voting procedures. The primary method of transmitting absentee balloting materials between the voter and local election offices is by mail. While this method works in most cases, it is a challenge to deliver balloting materials in a timely manner to a voting population that lives or serves in remote areas or distant places and/or is mobile (e.g., ships at sea, combat areas, missionaries and Peace Corps workers). Voters may not be able to receive their election materials by mail in a timely fashion if they are temporarily away from their place of residence, or in the case of active uniformed service members, away from their current duty station on temporary duty assignment, or who receive a permanent change of station in the weeks before an election.

Previous and Ongoing Electronic Voting Projects

The Department of Defense has a successful history of pursuing the use of electronic alternatives to the by-mail process of absentee voting, in order to ensure that all *UOCAVA* citizens have the opportunity to register and vote absentee regardless of their location. Often electronic voting alternatives provide a last resort for citizens faced with time, distance and mobility circumstances that could otherwise lead to his or her disenfranchisement.

Electronic Transmission Services (ETS)

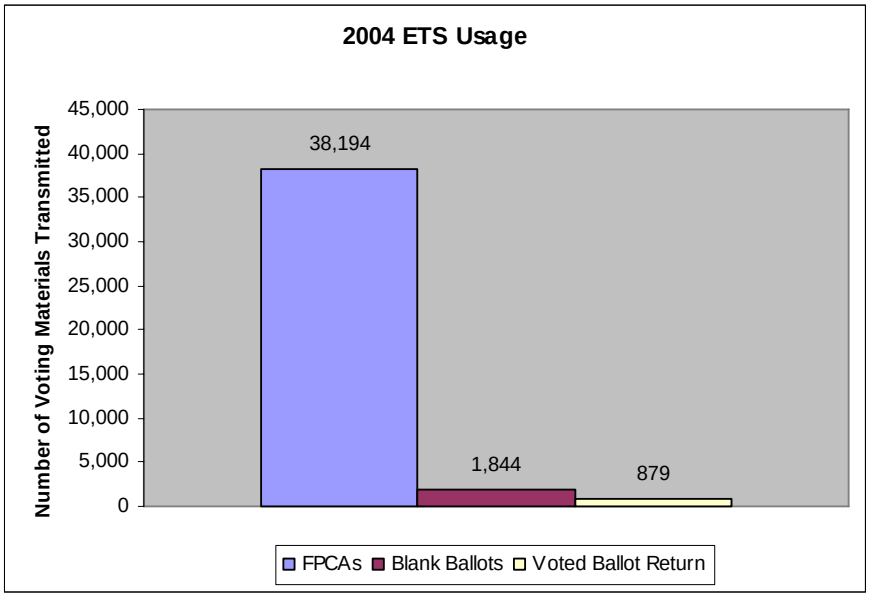
When military personnel were deployed for Operation Desert Shield in 1990, it was not possible to use the normal procedures for absentee voting for all personnel, since round trip transit time for mail delivery of election materials exceeded the time available to vote absentee in the election. In response, the Department, in cooperation with the states and territories, established the Electronic Transmission Service (ETS), which allowed deployed citizens in the Persian Gulf to request and receive their blank absentee ballots and return their voted ballots via fax. This system, during a two-month period, allowed for the transmission of 1,675 blank ballots to Service personnel serving in the

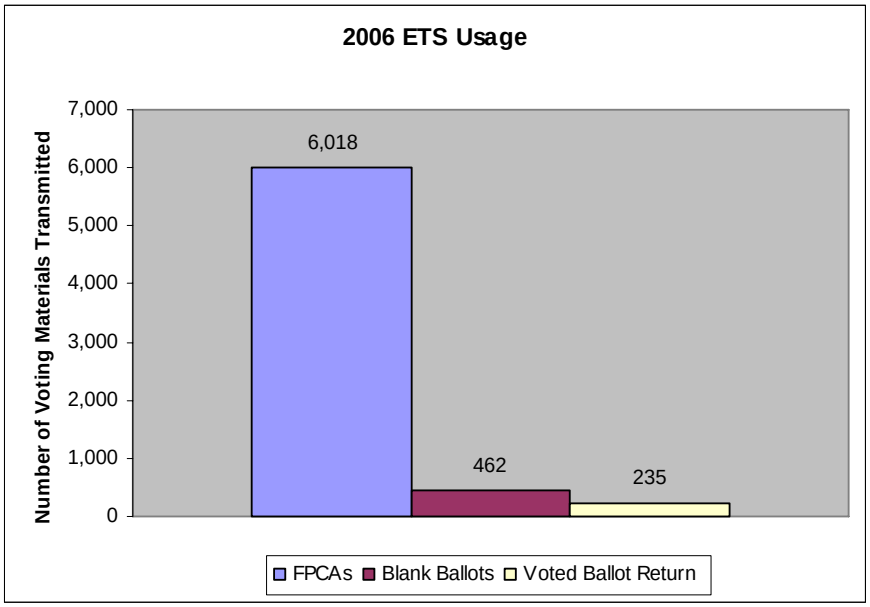
Middle East. The FVAP has continued use of the ETS and many states and territories have legislatively or administratively made changes in their election laws to provide for this method of transmitting election materials for *UOCAVA* citizens.

In October 2003, the FVAP expanded the ETS capabilities to include fax-to-email conversion in support of the uniformed services members stationed in Iraq and Afghanistan. Since faxing is limited in this region, email was presented as a viable alternative to service members stationed in this region. The ETS system established an email account as an option for voters and states to transmit election materials and absentee ballots. Some states did not allow election officials to email ballots directly to absentee voters, but their laws did allow the official to fax to the ETS. With the state's consent, the ETS would then convert the fax to a PDF attachment that could then be transmitted and received by the voter by email. The voter would print and vote the ballot, scan and email the completed ballot to the ETS, which would convert the email to a fax and transmit the ballot in fax format back to the local election official.

Currently, the ETS exists as a toll free option that allows local election officials and many voters to send and receive (where permitted by state law) applications for absentee ballots, blank ballots, voted ballots and other official election materials. Voters have the ability to send and receive absentee balloting materials through toll free fax numbers in 51 countries. The FVAP website includes links to the international toll free fax numbers associated with the ETS service. (http://www.fvap.gov/services/faxing.html)

The ETS service and cooperative efforts by the FVAP and the states to allow faxing of voting material and responses to voter queries have helped *UOCAVA* voters enormously. For the 2006 mid-term election the ETS transmitted 6,018 FPCAs, 462 blank ballots from local election officials to citizens, and 235 voted ballots from citizens to local election officials. In the 2004 general election, 38,194 FPCAs, 1,844 blank ballots, and 879 voted ballots were transmitted via the ETS.





Voting Over the Internet Project (VOI)

In 2000, the FVAP implemented the Voting Over the Internet (VOI) Pilot Project for use in the November 2000 general election. The goal of this small scale project was to examine the feasibility of using the Internet as an alternative method for remote absentee registration, ballot request, and voting for *UOCAVA* citizens. As changes in the voters' physical location are transparent when using the Internet, the VOI system was able to mitigate some of the time, distance and mobility issues experienced as it enabled citizens to register and/or vote regardless of where they had physically moved since requesting a ballot.

Security has always been a primary concern in the development of information technology systems that facilitate the election process for *UOCAVA* citizens. VOI was a proof of concept project and addressed these concerns rigorously through the use of digital certificates and encryption to provide privacy and security for all citizen and local election official transactions. The utilization of Department of Defense (DoD) Medium Assurance Public Key Infrastructure (PKI) as a separate system that managed digital certificates and certificate revocation lists provided for identification, authentication, non-repudiation, integrity and confidentiality for all PKI enabled DoD applications. Intrusion detection systems and independent test and certification processes were also applied.

Participating state jurisdictions were Florida, South Carolina, Texas, and Utah. The states of Florida, Texas and Utah designated specific counties to participate; the state of South Carolina chose to make the Pilot available to any *UOCAVA* citizen eligible to vote in the state.

The VOI Pilot Project provided the first opportunity for binding votes to be cast over the Internet in a general election for federal, state, and local offices. In 2003, the FVAP received the Excellence.Gov award for the VOI project from the Federal Chief

Information Officers Council and The Industry Advisory Council. The Caltech/MIT Voting Technology Project rated the VOI voter registration application a best practice for elections. VOI has served as a model of secure voting technology for similar electronic voting projects undertaken by the FVAP. The full VOI report is available on the FVAP website at http://www.fvap.gov/services/voi.html.

Secure Electronic Registration and Voting Experiment (SERVE)

Section 1604 of the *National Defense Authorization Act for Fiscal Year 2002* (Public Law 107-107) directed the Secretary of Defense to carry out a demonstration project that would enable absent uniformed service voters to cast ballots through an electronic voting system in the 2002 or 2004 general election. In 2002, The Director, FVAP, established a project management office to manage the Secure Electronic Registration and Voting Experiment (SERVE) for 2004. The objectives of the project were twofold: 1) to assess whether the use of electronic voting technology could improve the voting participation success rate for *UOCAVA* citizens and 2) to assess the potential impact on state and local election administration of an automated alternative to the conventional by-mail process of absentee registration and voting.

The FVAP worked with 7 volunteer states to develop a large scale, integrated, secure, web-based registration and voting system for use in the 2004 elections. This system envisioned allowing the voter to register and vote using any computer with Internet access anytime and from any location. It would allow the voter to register from one physical location and vote from another without having to notify his/her election official of a physical address change by mail. Other components of the system design which could be incorporated into existing state systems if the state desired, included delivering the correct ballot style to the voter; ensuring ballot design integrity; accurately capturing voter intent and voter ballot verification; and maintaining ballot secrecy. To provide a high degree of protection, the SERVE security design relied on multiple layers of redundant checks and balances throughout the hardware, software, and human elements of the system. Disaster recovery strategies were also incorporated. As an enhancement of the technology developed for VOI in 2000, the SERVE technology included roaming digital certificates for voter identification and authentication so the voter did not need a smart card enabled computer. Encryption mitigated the threats to network security and voter privacy. Digital signatures were incorporated to combat voter fraud, and controls were used to guard against vote buying and coercion. The FVAP developed extensive testing, implementation and post-election evaluation strategies that would serve to determine whether the SERVE project had satisfied its original objectives.

In the interest of transparency, and to glean constructive criticism to help improve the system security prior to deployment, the FVAP established a SERVE peer review group comprised of 10 members from academia and industry. A minority membership of this group independently publicized security concerns regarding the use of the Internet for the transmission of balloting materials. Responding to these concerns, then-Deputy Secretary of Defense Paul Wolfowitz decided that the SERVE project would not be implemented as planned. In a January 30, 2004 memo, he noted that the Department

"may continue efforts to demonstrate the technical ability to cast ballots through the use of electronic voting systems. These efforts should be designed to allow the Department to benefit from the work already in progress." Subsequently, the *National Defense Authorization Act for Fiscal Year 2005* authorized the delay of implementation of the electronic voting project providing that "the Secretary may delay the implementation of such demonstration projects until the first regularly scheduled general election for Federal office which occurs after the Election Assistance Commission (EAC) notifies the Secretary that the Commission has established electronic absentee voting guidelines and certifies that it will assist the Secretary in carrying out the project." The EAC will be working with the National Institute of Science and Technology (NIST) to develop these guidelines, and the FVAP will utilize these guidelines in the development of future electronic absentee voting projects.

While not taken to its intended conclusion, the SERVE project yielded useful information for the design and certification of electronic registration and voting systems, and for the direction of future innovation in the absentee voting process. The peer group minority report commented, "We want to make it clear that in recommending that SERVE be shut down, we mean no criticism of the FVAP, or of Accenture, or any of its personnel or subcontractors. They have been completely aware all along of the security problems we described, and we have been impressed with the engineering sophistication and skills they have devoted to attempts to ameliorate or eliminate daunting security problems. We do not believe that a differently constituted project could do any better job than the current team."

The following chart illustrates the maturity of the SERVE project security.

Threat	Mitigation
Network Security	- Encryption - Intrusion Detection Systems - Redundant Firewalls - Penetration Tests
Privacy	- Digital Signatures - Secure Socket Layers - Encryption - Voter Identity—Ballot Data Separation - Voter Ballot Data Verification
Virus, Worm, Trojan Horse	- Anti Virus Scanning - Digital Signatures - Voted Ballot Data Verification
Spoofing	- Secure Socket Layer - Digital Signatures - Voted Ballot Data Verification
Denial of Service	- Large Quantity of Bandwidth, Multiple Carriers - Multiple Internet Service Provider Entry Points - Utilization Monitoring
Voter Fraud	- Digital Signatures

Encouraging State Initiatives

The FVAP has consistently encouraged the states and territories to develop electronic transmission alternatives independently, particularly after the SERVE project was discontinued. Because of legislative initiatives developed by the FVAP urging all the states and territories to adopt these technologies, email and faxing protocols are becoming more widely available to *UOCAVA* citizens as alternatives to the by-mail absentee voting process. Fax and email options for voter registration, request and delivery of blank ballots, and voted ballot return greatly reduce the amount of time needed to complete the process, and enfranchise *UOCAVA* voters by providing additional alternatives when regular mail may not reach the citizen due to his or her remote location or unreliable mail service in the country where they reside. Currently:

- 32 states and territories allow *UOCAVA* voters to submit the Federal Post Card Application for registration by fax.

- 51 states and territories allow *UOCAVA* voters to submit the Federal Post Card Application for absentee ballot request via fax.

- 36 states and territories allow *UOCAVA* voters to receive the blank ballot via fax.

- 24 states and territories allow *UOCAVA* voters to return the voted ballot via fax.

Many states and territories have expanded their electronic transmission alternative capabilities to include email. Since many forward deployed soldiers have email capabilities but do not have access to fax machines, the ability to use processes that allow for email ballot request, ballot delivery, and/or ballot return can be crucial. Some email protocols are provisional as noted. Currently:

Six states allow *UOCAVA* voters to submit the Federal Post Card Application for registration via email:

- Alaska
- Oregon
- Mississippi (for active duty overseas)
- Montana
- Washington
- West Virginia

Twelve states and territories allow *UOCAVA* voters to submit the Federal Post Card Application for absentee ballot request via email:

- Alaska
- Illinois (City of Chicago and Cook County only)
- Montana
- Minnesota (restricted)
- Mississippi (for active duty overseas)
- North Dakota
- Oregon
- Puerto Rico
- South Dakota
- Washington
- West Virginia
- Wisconsin
- (Iowa allowed for 2006 election)

Thirteen states allow *UOCAVA* voters to receive blank ballots via email:

- Alaska
- Colorado (uniformed service members outside the U.S. via ETS.)
- Florida
- Illinois (City of Chicago and Cook County only)
- Montana
- Mississippi (for active duty overseas)
- North Dakota
- Oregon
- South Carolina
- Virginia (certain counties only; uniformed service members outside the U.S.)
- Washington
- West Virginia
- Wisconsin
- (Iowa allowed for 2006 election)

Seven states allow *UOCAVA* voters to return the voted ballot via email:

- Alaska
- Colorado (uniformed service members outside the U.S. via ETS)
- Mississippi (for active duty overseas)
- Montana (certain counties only)
- North Dakota
- South Carolina
- West Virginia
- (Iowa and Missouri allowed for 2006 election)

Four states and territories currently do not allow any form of electronic transmission of voting material:

- Alabama
- Guam
- New York
- Wyoming

IVAS 2004

The Interim Voting Assistance System (IVAS) was a project the Department voluntarily deployed in September 2004 to allow eligible absentee voters to request and receive their absentee ballots via the Internet. In order to take advantage of IVAS, voters must have already been in the Defense Enrollment Eligibility Reporting System, be a U.S. citizen covered under *UOCAVA*, and must have been registered to vote in a participating county.

Using IVAS, the voter could request a ballot via a secure connection to a dedicated website. After the local election official approved the request, IVAS notified the voter via email that the ballot was available to download. The voter could then download and print the ballot, mark it by hand and return it by mail to the local election official. One hundred eight counties in 9 states permitted the use of this alternative method in 2004 with 17 voters utilizing it to download ballots.

IVAS 2006

IVAS 2006 was an electronic alternative information, ballot request, and delivery site implemented by the Department of Defense to serve citizens covered by *UOCAVA.* It was launched on September 1, 2006 for use in the November 2006 general election. Made available through the FVAP website, the renamed Integrated Voting Alternative Site (IVAS) provided expanded coverage via consolidated information from the 55 states and territories on electronic transmission alternatives for ballot request, blank ballot delivery and voted ballot return for citizens covered by *UOCAVA.* Additionally, IVAS provided two tools to the states for blank ballot request and delivery. Eleven states and territories opted to use one of the two tools. Access to either tool required a unique DoD identifier possessed by uniformed service members, their family members, and overseas DoD employees and contractors. For this reason, use of the two IVAS tools was limited to this sub-population of *UOCAVA* citizens.

Tool One allowed *UOCAVA* voters previously registered to vote in a participating jurisdiction to request an absentee ballot via email. It was utilized by 470 jurisdictions in 8 states. Between September 1, 2006 and November 7, 2006 the automated FPCA associated with Tool One was accessed 1,351 times. Because users of IVAS Tool One submitted their FPCA ballot requests directly to local election officials using their personal email accounts,

the FVAP does not know the number of absentee ballot requests actually submitted using this tool.

Tool Two allowed for ballot request and blank ballot delivery through a secure server for voters registered to vote in a participating jurisdiction. Tool Two also had the capability to allow the voter to be notified that the LEO had received their mailed, voted ballot. It was used by 103 jurisdictions in 3 states. Between the September 1, 2006 IVAS launch date and November 5, 2006, the IVAS section of the FVAP website received 34,857 hits; 147 voters successfully logged into the system and 63 ballot requests were submitted. Of those, 35 ballot requests were approved; 14 requests were denied; 9 requests were deferred and 5 requests were not processed. (A request might not have been processed if, for example, it was sent to the wrong jurisdiction, was received too late, or, as was the case in Indiana, where a "wet" signature was required and the original signed document did not arrive in time to be processed). Of the 35 ballots approved and sent to voters, 29 were viewed by the voters.

The FVAP and Post X, the IVAS Tool Two development sub-contractor maintained help desk operations to field questions from local election officials and *UOCAVA* voters.

EXPANDING THE USE OF ELECTRONIC ALTERNATIVES FOR FUTURE ELECTIONS

The FVAP's goal is to provide as many options as possible for local election officials to communicate with the citizens they serve, and to meet the real world situations faced by *UOCAVA* citizens. In an FVAP survey immediately following the 2006 election, most local election officials indicated that they would like to continue the use of IVAS in future elections. Responding to the needs of the states and territories, and *UOCAVA* citizens, the FVAP will continue the promotion of electronic transmission alternatives to the by-mail absentee voting process. During the planning process for 2008, technologies have been and will continue to be examined for their efficacy as well as their potential vulnerabilities. FVAP considerations include lessons learned from the 2006 election as well as observations from the participating states, recommendations from other federal agencies, and the technologies already in use in the 55 states and territories and other countries.

Lessons Learned from State and Voter Experience with IVAS 2006

Post-Election Survey of Local Election Officials – IVAS Tools

Immediately following the November 2006 election, the FVAP conducted a written survey of local election officials on both their quantitative and qualitative experience with the two IVAS tools. Among the data solicited were the total number of ballot requests received via IVAS, number of ballots sent to voters who requested ballots via IVAS, and number of voted ballots received from voters who had requested ballots via IVAS. Additionally, local election officials were asked to comment on their overall experience in terms of ease of use, effectiveness of training, quality of assistance, and whether they would like to continue the use of IVAS in future elections. Participation in the IVAS survey by state election officials

was voluntary, so data gathered by the FVAP on IVAS 2006 may be representative, but is not definitive and cannot be projected.

Tool One Survey Observations

Surveys were sent to 470 participating jurisdictions and 22 completed surveys were returned. Of these, 19 indicated that they would like to use IVAS in future elections. An official from one large jurisdiction commented that voters were surprised to receive their ballots so quickly and that IVAS "opened a line of communication with the voters that is invaluable in the process". Election officials who contacted the FVAP help desk with questions reported that their questions were quickly and satisfactorily addressed. No respondents indicated that they had any technical difficulties facilitating the emailed ballot request received via IVAS using Tool One.

Tool Two Survey Observations

Surveys were sent to 103 participating jurisdictions and 24 completed surveys were returned. Fourteen officials indicated that they would like to continue the use of IVAS in future elections. Ten respondents indicated that they would not and cited the following reasons: lack of time to learn the procedure; the tool required too much technical expertise; the set up was confusing; they did not receive passwords in a timely manner; and that its use fell outside their regular workflow and for that reason they never really became comfortable with it.

Conference Calls with States Regarding their 2006 IVAS Experience

In January and February of 2007, the FVAP conducted conference calls with election officials from states that participated in the two IVAS tools. Although all Tool One participants found the email protocol to be convenient and straightforward, none felt that the tool was widely used. All expressed an interest in using the same or similar tool in future elections, and were consistent in their desire to have tools available much earlier in the election cycle in order to promote its value to both local election officials and *UOCAVA* voters.

The three state officials that utilized Tool Two were equally committed to participating in some form of the IVAS tools in future elections and had specific comments about the benefits of the tool and the challenges they perceived moving forward. Because Tool Two utilized a secure server requiring a log-in procedure, it was somewhat more complex than Tool One.

Kentucky officials expressed frustration that the tool was made available too late in the election process. Local election officials did not have enough time to become familiar with the ballot request and delivery process. They also cited a lack of infrastructure in the counties (e.g., access to email) and a lack of familiarity with the technical requirements of the tool (accessing and forwarding ballots in PDF format) in some jurisdictions. Kentucky

officials indicated that they expected their electronic communication infrastructure to be more fully in place for the 2008 elections.

Indiana utilized Tool Two, but state law required that the voter submit a signed copy of the FPCA ballot request via fax, regular mail, or fax-to-email capability of the FVAP's Electronic Transmission Service. The voter could use the Tool Two secure server to request the ballot, but could not receive it via the server until a signed ballot request had been received by the local election official. Indiana officials cited this legal requirement as a demonstrable need for flexibility in future ballot request and delivery tools.

Montana officials, who also utilized Tool Two, observed that for the 2006 election local election officials were already challenged by implementing new systems mandated by the *Help America Vote Act* of 2002 (*HAVA),* and simply did not have time to learn and employ an additional system. Some were skeptical that the new protocol was secure, accountable and complied with state law, and were therefore reluctant to become involved in the process.

These conversations with the states that participated in IVAS served to reinforce the FVAP's desire to implement ballot request and deliver tools that are flexible, convenient and as secure as possible based on risk analysis, and that any system or suite of tools needs to be established and made available to the states as far in advance of the election as possible. To encourage broad participation by the states, and robust *UOCAVA* voter activity, the FVAP needs several months after any new tool is designed to develop training materials, and train and educate users in state and local election offices, particularly when the project involves processes that may be different form the existing state and local election official practices. The states and territories need many months to reach out to their local election officials. The FVAP and the states and territories also need time to reach out to *UOCAVA* citizens, so they can be made aware of the alternatives available should the by-mail process not work for them. Adequate lead time will be particularly important for the 2008 presidential election, as voter interest is historically greater for presidential elections than it is for mid-term elections.

Previous experience with electronic remote voting systems has made it clear that the development process alone requires time to design, test, evaluate, train users, and deploy new technology, as well as incorporate improvements and lessons learned into subsequent versions.

Observations by Other Agencies

Both the EAC and the Government Accountability Office are currently conducting studies on *UOCAVA* electronic voting alternatives. The FVAP will take their results and recommendations into consideration as it continues to develop products for use by the states and territories, and *UOCAVA* citizens in 2008 and 2010.

Electronic Voting Technologies in Other Countries

As the DoD moves forward in the development of electronic voting technologies for *UOCAVA* citizens, the FVAP is evaluating lessons learned from IVAS, from its previous electronic voting projects, and from efforts undertaken independently by the states and territories. In addition, other nations have begun to investigate and test the use of remote electronic voting tools for their citizens. Several of these projects are summarized below.

Canada

During November 2004 elections in 12 municipalities in Ontario, Canada, about 100,000 voters registered to cast ballots online or by touch-tone phone using an assigned Voter Identification Number and a password. This electronic voting effort increased voter participation from the normal rate of 25-30% to 55% in some places. (Source: ACE Electoral Knowledge Network)

England

In May of 2003, pilot programs in England took place in 59 local jurisdictions. Approximately 6.4 million people were eligible to vote in these pilots via a variety of channels – on the internet, by telephone, via text messaging and through interactive digital television. Similar electronic strategies were to have been used in local elections in May 2006 but were subsequently abandoned, primarily over concerns about the lack of an adequate audit trail. Electronic trials continue cautiously. In May 2007, elections in 6 local jurisdictions allowed voting over the internet. Five of these jurisdictions also utilized telephone voting. One of the advantages of these electronic alternatives is that they allow voters a wider timeframe in which to act, with lines open for 4 days (3 days prior to Election Day, and on election day itself). (Sources: World E-gov Forum; *The Independent*; European Digital Rights EDRI.org; ACE Electoral Knowledge Network)

Estonia

The technologically favorable infrastructure of Estonia strongly supports the possibility of internet voting. It is the only country in Europe where access to the internet is legislated as a social right.

The Estonian internet voting system has been under development since a legal provision supporting it was put into place in 2002. In part, the effort was undertaken to combat falling voter turnout and to bring young, tech-savvy people back into the voting pool. Internet voting is offered in conjunction with traditional voting methods and has been introduced primarily as a convenience and an improvement on postal voting systems already in use. The Estonian company Cybernetica, Ltd. developed the system, which uses smart cards and electronic signatures.

Once the legal issues surrounding internet voting were satisfied, the Estonian National Election Committee determined that there were no technological obstacles.

Significant modifications were implemented to increase security after hackers tested the system for vulnerabilities in various trial runs. Primary modifications included: the disconnection of several subsystems; police protection of the servers; and disconnection from the internet of the computer that processes the votes.

The software was tested in a small scale referendum vote in the city of Tallinn in 2004 and was taken nationwide for local government elections in October of 2005. This was the first time that an electorate of an entire country could cast its vote over the internet in a public election. Internet voting took place over a 3-day period prior to the October 16, 2005 election day; 9,317 voters participated (1.85 percent of participating voters, in an election with a 47.4 percent voter turnout).

The internet voting procedure required a government issued electronic ID card equipped with a computer–readable microchip and digital signature that allowed the voter to be unambiguously identified online after logging on to vote. More than 80% of Estonia's 1.06 million registered voters have these ID cards. However, in order to participate in the election voters needed to have the card validated for use online and had to purchase an ID card reader for approximately $15 which required software that some critics regarded as difficult to install on laptops and PCs. The encrypted system was based on the digital envelope method and used public key cryptography.

The system allows for electronic re-votes. The voter can cast his or her ballot again electronically and the previous vote will be deleted. Should the voter go a polling station during the advance voting period and vote in person, any prior electronic vote will be deleted. On Election Day registered electronic votes cannot be changed or made void. At the end of the advance election period, a list of voters who have voted electronically is compiled and sent to polling stations. The station makes a notation on the voter list that the person has already voted. This prevents them from voting for a second time on election day. A benefit of the reversible internet voting mechanism is that it has potential for overcoming fears of vote buying and coercion in respect to remote voting by allowing voters to re-cast ballots that may have been coerced.

Observers from approximately 40 countries witnessed the process. Election observers noted no technical problems and no hackers were detected manipulating the process. The electoral commission did not receive any complaints following the election regarding the e-voting system. A post election survey indicated that internet voting was perceived as convenient and that it made voting quick, practical and overall simplified. Detractors point out that although Estonia has issued more than one million of the necessary ID cards, relatively few of the nation's computer users have installed the smart card readers that accept them. Further, the system leaves no traditional paper trail for election observers to follow.

The October 2005 internet voting experiment was deemed a success. The process was used again in national parliamentary elections in March of 2007 when 30,275 votes were cast over the internet. (Sources: World E-gov Forum; Euractiv.com; ACE Electoral Knowledge Network; UBINS.org)

The Organization for Security and Co-Operation in Europe (OSCE) observed the March 2007 elections. The OSCE findings have not been released as of this report's issuance.

France

French citizens living in the United States were allowed to elect their representatives to the Assembly of French Citizens Abroad (a public legislative body which elects members of the Upper House of the French parliament who represent French citizens residing abroad) in June of 2003, over the Internet using CyberVote, a highly secure and encrypted voting solution developed by EADS Defense and Security Systems. Following that experiment, the Internet Rights Forum, a private board supported by the French government recommended that electronic voting should not be introduced to the general citizenry, but that it should continue to be available to French citizens abroad. Elections for this population were subsequently held on June 18, 2006 with an eligible voter base of 525,000 individuals residing in 68 countries; 28,138 individuals registered to vote via the internet and 10,200 votes were cast. The relatively low participation was due, in part, to the complexity of the process. During the week before the election, the voter had to confirm his/her registration, and had to test his/her computer's compatibility with the protocol. (Sources: World E-gov Forum; European Digital Rights edri.org; ACE Electoral Knowledge Network; Internet Rights Forum)

The Netherlands

In the 2004 European Parliamentary election, 5,351 of the roughly 16,000 Dutch citizens who were living overseas, and who registered for remote electronic voting, cast their ballots via the Internet or over the telephone. During the development process it was recommended that the design, implementation and testing procedures should not be conducted by the same company. Testing was conducted by the Security of Systems (SoS) Group at Radbound University Nijmegen. SoS Group did not take part in either the design or implementation of the system, but did take an active part in performing a penetration test of the vote servers. SoS Group had virtually no knowledge of the hardware, software, networks or personnel involved with the server system. In fact, the information it did possess was essentially public information, since it could be easily obtained by readily available analysis tools. The testing goals comprised two scenarios: 1) to attempt to break into the system and compromise its integrity and 2) to see if the system was vulnerable to denial of service attacks. Testing revealed that the systems were appropriately hosted, monitored and configured, and that adequate measures were installed for detecting attack – no compromise to the system was detected. However, the system was easily stalled by a denial of service attack. Because this risk is virtually impossible to prevent completely, the Dutch Ministry accepted the system and proceeded to utilize it in the overseas election.

Along with standard security protocols, the Dutch remote voting system included some interesting features: 1) Data integrity was ensured by the use of candidate codes. 1,000 codes were generated for each candidate and only one of these codes was randomly assigned to each voter. Consequently, it was virtually impossible for an attacker to substitute the ballot by choosing the appropriate code for a different candidate; 2) votes were doubly encrypted.

The only opportunity to decrypt the votes on the server side would be to close the polls. As closing the polls was an irreversible action, altering the votes at the server side was not possible; 3) if a voter tried to utilize both technologies (phone and internet) to cast a vote, only the first vote was stored. The second attempt would fail because the voter had already cast his or her vote; 4) voters were able to verify that their ballot had been correctly recorded and included in the final election tally by using a transaction code they received when casting their ballots. The evaluation of the experiment determined that a large number of voters abroad considered that Internet voting had an added value and made voting more accessible, and they would like to have the option of voting on the Internet again in the future. For the November 22, 2006 Parliamentary elections, Dutch citizens overseas had their choice of voting over the Internet or the traditional by-mail method. For 2006, the transparency of the system had been improved, the registration and authentication process had been made more voter-friendly, the voting period was shortened and telephone voting was not available. A thorough post-election evaluation is being conducted, the results of which will be used in a political debate about the use of Internet voting in the future. (Sources: ACE Electoral Network; Ministry of the Interior and Kingdom Relations "Evaluation Report; Experiment with Internet and Telephone Voting for Voters Abroad")

New Zealand

In the July 2002 general election the New Zealand Chief Electoral Office introduced to its overseas voters an electronic voting alternative much like 2006 IVAS Tool Two. Voters logged onto a secure server using shared secret identifiers to request and download ballots. Ballots were then printed, marked, signed and faxed back to the Election Office. The service was well received by voters – approximately 20,000 participated, and there were no reported disruptions or instances of hacking. (Source: ACE Electoral Knowledge Network)

Spain

In November 2003, a non-binding remote electronic voting pilot was run parallel to the public election. More than 23,000 Catalan citizens residing in Argentina, Belgium, the United States, Mexico and Chile were invited to participate in the election using any computer connected to the Internet by means of a web browser supporting Java (virtually 100% of the browsers on the market). Java technology was required to cryptographically process every individual ballot to ensure its security. Participants logged onto the system using credentials that had been mailed to them and 730 ballots were cast. Subsequent voter opinion surveys showed clear approval of the system; 97% were satisfied or very satisfied with the experience; 96% found that the system gave much or a reasonable amount of confidence; 98% found the system easy or very easy to use; and 98% indicated that they definitely or probably would have chosen to use the system if the process would have been binding. Subsequent evaluation of the process, including the inherent risks discussed previously in this report concluded that electronic voting has the potential to improve the electoral experience and enhance the democratic process, but that naively implemented electronic voting systems can pose serious threats to the integrity of elections and shake public confidence. Sophisticated security measures are clearly required to maintain the public trust. (Source: ACE Electoral Knowledge Network)

Switzerland

In August of 2000, the Swiss government began examining the possibilities of electronic voting for citizens living away from their polling places. From 2003 to 2005 a variety of legally binding test projects were conducted in the canton of Geneva, the communities of Anieres, Colony, Carouge, Meyrin, Neuchatel and Zurich. The Swiss government and parliament used the pilot projects to determine the future of remote electronic voting as a supplementary vote counting method. The system is based on existing voting materials and requires no added features on the voter's computer (e.g. ID card reader). Registered voters receive polling cards and ballots by regular mail prior to each election. The polling cards contain a voter number as well as a secret identification code that is printed under a scratchable metallic strip. To vote electronically, the voter access the e-voting system through the internet, enters his or her voter number and enters his or her ballot choices. Upon confirmation of those choices, the voter enters the secret identification code, along with date and place of birth. The system then confirms that the vote has been successfully transmitted and recorded. Polling cards on which the metallic strip has been scratched off may not be used in person at polling places or for ballots returned by mail unless a barcode check indicates that the voter has not previously cast a vote electronically. (Sources: ACE Electoral Knowledge Network; World E-gov Forum; "The Scope of E-Voting in Switzerland", Daniel Braendli, Swiss Federal Chancellery)

Electronic Voting Technologies in the States

The 55 states and territories have been resourceful in expanding alternative electronic transmission capabilities (particularly fax and email) for voter registration, ballot request and blank ballot delivery, and for several years the FVAP has been encouraging these advancements through legislative initiatives. Beginning with the VOI project in 2000, and continuing to date, the FVAP has also encouraged the state governments to expand their acceptance of digital signatures for registration and voting purposes. One of the principal requirements for the VOI project was to be able to identify and authenticate voters with a high degree of certainty. The mechanism selected to provide this capability was the DoD Medium Assurance PKI. The issuing procedure for digital certificates required the recipient to appear in person before an issuing authority or the authority's trusted agent and present official photo identification. The use of digital identifiers throughout government continues to grow. Homeland Security Presidential Directive 12, announced on August 27, 2004, mandates the use of "smart cards" which contain electronic credentials that allow their bearers to be identified in several ways – photographic images, fingerprints, personal information numbers, and digital signatures. As the government agencies fulfill their obligations to provide these cards to government personnel, the number of individuals possessing these electronic identifiers has grown considerably. Currently approved for use in many states for banking, insurance and commerce-related transactions, digital signatures (as used in the FVAP's VOI project) are not yet employed in the elections process. (Utah did authorize electronic signatures attached to voted ballots for the 2000 FVAP VOI project to be used for identification and authentication of voters). The FVAP believes that the ability to use these electronic identifiers on balloting material would be an enormous benefit as an

alternative method for those *UOCAVA* citizens who possess them, and the FVAP continues to work with the states to apply the use of this technology to the elections process.

Currently, approved technologies for voter registration, ballot request, blank ballot delivery and voted ballot return may include fax and/or email, however there are considerable differences among the states and territories as to which technologies are accepted and which parts of the voting process may utilize electronic transmission. At the present time 3 states and 1 territory do not allow any form of electronic transmission. In the 2006 general election, 7 states allowed voted ballots to be returned to election officials by email. Additionally, the states of Washington and Florida allow registered voters to request blank ballots by phone, and Kentucky allows phone requests for its military voters.

Electronic systems are facilitating the election process for voters and election officials in other ways. In Michigan voters can check their registration status online and registered voters can view their appropriate ballot. Any citizen, from any location, can access the system without the need for digital signatures or other credentials. 24 states have similar capabilities on their websites.

The State of Washington is using electronic ballot tracking. Available to all 39 counties, the system allows election officials to track every ballot from the time it is mailed to the voter to the final vote tally. A list of voter names is produced at each step of the ballot handling process and the system permanently separates and randomizes voter names from ballot barcodes to protect voter privacy. Reports alert election officials to ballots that have missed a step in the process. Voters can verify the status of their ballot online – when it was mailed, when the voted ballot was received by the county, when their signature was checked, when the ballot scanned, and when their vote was counted.

Multnomah County, Oregon, allowed *UOCAVA* citizens to request ballots via email for the November 2006 general election and provided these ballots as a back-up for ballot packages sent to them via regular mail. The emailed ballot packages included the appropriate blank ballot, the complete text of ballot measures, a self-addressed return envelope template to be folded and signed by the voter, along with instructions for completing and returning the voted ballot by mail. State law does not currently allow for voted ballots to be returned by email. Any registered *UOCAVA* voter could request a ballot by email, and no credentials needed to be submitted at the time of the request. Voter registration cards are scanned and the signatures are available electronically in the county's Election Management System. The signature on the return envelope was compared against the electronic record to authenticate the ballot. If the signature did not match and the discrepancy could not be explained by the voter, the envelope was not opened and the ballot was not counted. For the 2006 election, 99 ballots were issued via email. Twenty seven of these were returned as voted ballots; more than 50 other voters returned their original, mailed ballots. A Multnomah County election official reported that their primary challenge was obtaining United States Postal Service approval of the return envelope design. Once accomplished, Multnomah County assisted 4 other Oregon counties to gain envelope design approval so that they, too, could assist *UOCAVA* citizens via email. The protocol was adapted from a process used in Pierce

County, Washington. Several other Washington counties provide this email ballot request service to its *UOCAVA* citizens.

Also new during the 2006 election was a vote-by-phone system utilized by the states of Connecticut, Maine, New Hampshire, Oklahoma, Oregon, and Vermont. It was developed to assist disabled voters to cast ballots independently and privately in their polling places. The Director, FVAP, viewed a demonstration of the Vermont vote-by-phone systems for possible future application for remote use by *UOCAVA* voters. In its current application, the voter uses an identification number to access the appropriate ballot. The ballot is read over the phone and the voter uses the telephone keypad to indicate their selection. A paper ballot of the vote is printed at the office of the Secretary of State, providing a paper trail for auditing purposes. At present, the system relies on dedicated land line telephone access and will not function with cell phones and denies access to any unknown phone number. In a post-election discussion with the FVAP, Vermont Secretary of State Deborah Markowitz noted that they were pleased with the phone voting project and that the state would continue its use for serving their disabled citizens in polling places but has no immediate plans for expanding its use to other populations or venues. While limited in scope and accessibility in 2006, telephone voting remains an interesting technology, and one worth exploring for its benefits not only to disabled voters, but to *UOCAVA* voters.

Although there are risks associated with voting over the internet, several states have independently launched relatively small scale pilot programs to investigate its potential. Certainly the accessibility of this alternative, particularly for *UOCAVA* citizens, merits continued consideration. Voter participation was vigorous in these experiments, suggesting that voters both trust the security of the internet and enjoy the convenience it provides.

Michigan allowed online voting in its Democratic presidential caucus in 2004. The result was the second largest caucus turnout in state history; of the 164,000 total votes, 46,000 were cast online. Arizona used internet voting in its 2000 Democratic primary, experiencing larger than usual voter participation.

The City of Honolulu offered a small scale internet voting pilot project in March 2007 for neighborhood board elections. The goal was twofold – to provide cost-effective voter access and to increase voter turnout. Registered voters were allowed to vote from any computer with internet access using personal identification numbers that were either mailed to them on a printed ballot or were requested by voters on a voting website. Approximately 405,000 registered voters were eligible to participate in this internet voting pilot.

FVAP PLANS FOR THE ADVANCEMENT OF ELECTRONIC VOTING TECHNOLOGY

The FVAP anticipates that the 2008 general election will generate enormous public and media interest, resulting in larger than usual voter participation. Presidential elections historically garner more voter participation than that of mid-term elections, and, in recent decades, an incumbent President, or sitting or former Vice President has almost always been among the nominees of the Democratic or Republican parties. In 2008, it is likely that the

presidential election will be an open race, the first time since 1952 that neither a Vice President nor sitting President will be a nominee. It is expected that *UOCAVA* citizens will be eager to participate in this upcoming election and that the challenge of overcoming the obstacles to obtaining voting materials faced by these citizens will continue. As the Director, FVAP is charged with supporting this *UOCAVA* population in their voting efforts, the Department is aggressively pursuing the development of secure electronic voting processes with the states that will address these obstacles and help enfranchise *UOCAVA* voters.

Although issues of security dominate discussions of the development of electronic voting technologies, FVAP will consider a broad range of issues as it proceeds toward the elections of 2008 and 2010. Designing and developing a mature voting system takes a series of election cycles. There must be enough time to gather and analyze post-election data, as well as for training, and developing or updating the voting system to meet the requirements of federal, state, and local election official practices. The system design must consider many variables, including: security measures; the needs of *UOCAVA* voters; accessibility of the system's technology; federal, state and local election resources and regulations; and ease of use. As in VOI and SERVE, an incremental development, implementation and evaluation plan should be articulated at the beginning of future projects and milestones specified for each stage of the project.

Based on past practices and experience, recommendations for future electronic voting projects include: working up to a large scale system starting with a small number of states or limiting capabilities; recognizing the variation in state and local laws and procedures, and the complexity this introduces in the development of a uniform registration and voting system; building consensus of key stakeholders; identifying and mitigating actual and perceived risks by educating people about risk management practices; ensuring that the system will be testable and that those tests can be reproduced; standardizing the interfaces for the voting systems for easier interconnectivity; developing guidelines for electronic or internet-based registration, ballot delivery, and voting systems which maintain the integrity of the process; and assessing methods for voter identification and authentication involving digital certificate technologies.

In the interest of providing as many tools as possible for state and local election officials to select from based on their states' legal requirements, the DoD believes that multiple strategies should be developed and deployed. The process should explore the technological tools available beyond fax and email for use in remote electronic voting, among them touchtone telephone, text messaging, interactive television and the Internet. Creating a system that supports multiple platforms adds significantly to the complexity of the design and cost associated with development, testing and certification. Live election testing should begin on a small scale and increase in scope over a series of election cycles. All technologies should be examined for their efficacy as well as their vulnerabilities. The means to balance the provision of electronic alternative to those who most need them with the need for accuracy, reliability, privacy, security and transparency in the voting process, will have to be continuously re-evaluated and adapted.

LONG RANGE STRATEGIES

The Election Assistance Commission (EAC), in conjunction with National Institute of Standards and Technology (NIST) was assigned the task of developing electronic absentee voting guidelines by the *National Defense Authorization Act for 2005 (NDAA FY 05).* In 2007, the EAC is expected to release the results of a study of Internet voting and the transmission and receipt of absentee ballots for voters covered under *UOCAVA.* The study will include a review of the practices of voting jurisdictions that use technological alternatives to transmit or accept ballots and that may allow Internet voting, as well as a survey of *UOCAVA* voters who participated in some form of electronic voting. It is hoped that the study will effectuate further understanding of the problems and resource constraints, as well as potential solutions to meet *UOCAVA* voting challenges. It is the DoD's understanding that the results of the study will be used as a basis from which the guidelines will be developed. The DoD is prepared to work with the EAC on the study and guideline development. The release of the EAC recommended voting guidelines, as well as the insights provided by the study and from follow-up conferences of state and local officials from jurisdictions who participated in remote electronic voting will be utilized by the DoD as it pursues its legislative mandate to carry out an electronic voting demonstration project.

Dependent on the level of security called for in the EAC and NIST guidelines, the Department may pursue the development of an internet voting strategy mirroring the functionality and security that were contained in its previous VOI and SERVE projects, or of an enhanced IVAS allowing for the transmission of voted ballots. A complete internet voting system would provide the following functions: voter identification and authentication, voter registration, election administration, ballot delivery, voting, tabulation, and results reporting. Based on the recommendations included in the internet voting guidelines and the final design of the system, full development, testing and deployment would require an estimated 24 to 60 months. The successful deployment of any system also requires participation from the states as well as the Military Services, which have many competing priorities during this time of increased operations. Education and outreach efforts would also include local election jurisdictions, municipalities (if required), federal agencies, and overseas citizen groups. It is possible that a complete solution could be implemented incrementally; designed, tested and used with capabilities and features added over the course of several general elections. The following timeline shows the primary project tasks and the anticipated time needed for completion. Some tasks are dependent on previous phase completion while others can run concurrently.

Concept Development with high level requirements	180-360 days
Communications Plan	60 days
Contracting Process	80-155 days
Design Phase	100-200 days
Development Phase	400-700 days
Testing Phase (meeting Federal, DoD, and state security requirements)	150-230 days

ELECTRONIC VOTING PLANS FOR 2008 AND 2010

The required guidelines on electronic voting from the EAC and NIST will frame the strategies for the eventual development of a large-scale internet voting project that will most likely mirror the functionality and the security of the VOI and SERVE projects. The guidelines have not yet been released and this anticipated project is several years from inception. In the meantime, the FVAP will continue to provide voter registration, ballot request, and ballot transmission strategies that are alternatives to the by-mail process for *UOCAVA* citizens during the 2008 and 2010 election cycles. The Department will not offer any tools that allow for voters to cast voted ballots over the internet. If any states, territories or localities do offer such a service, the DoD will assist in publicizing the ability for the effected voters.

For 2008 and 2010, the FVAP anticipates continuing and enhancing key elements of its efforts from 2006. These include: an improved FVAP website which provides consolidated information for *UOCAVA* voters from the 55 states and territories on electronic transmission alternatives allowed for ballot request, and blank ballot delivery and voted ballot return; and access to the automated FPCA for voter registration and absentee ballot request. Additional capabilities will include a tool for automated population of the FPCA that is mapped to specific absentee voting requirements for the 55 states and territories similar to those developed and utilized by the DoD in the VOI project in 2000, and designed for the 2004 SERVE project. An automated version of the FPCA will assist voters while they navigate the form, and ensure that *UOCAVA* citizens complete the FPCA in accordance with their state laws and procedures. Voter error while completing the FPCA can compromise the absentee voting process. If a local election official receives an incomplete or incorrect FPCA, the citizen must be notified and must resubmit the FPCA. If this process is performed entirely via regular mail, it may take weeks or months before the voter is made aware of the mistake, and may not have enough time to resubmit the FPCA and receive a blank ballot to complete and return by their state's election deadline.

In addition, the FVAP and the states and territories will maintain the toll-free Electronic Transmission Service. The ETS provides thousands of *UOCAVA* citizens worldwide with fax and fax-to-email alternatives to the by-mail process of absentee voting.

The FVAP will also continue to promote its legislative initiatives with the states, encouraging the expansion of electronic alternatives for *UOCAVA* citizens who live and serve in remote areas or distant places and are mobile (e.g., ships at sea, combat areas, missionaries and Peace Corps workers).

Additional enhancements under investigation for use by the states and *UOCAVA* citizens in 2008 and 2010 may include enhanced ballot tracking (to inform voters that his or her voted ballot has been received and counted), and a function that would allow absentee voters to check and correct, if necessary, their mailing address for voting materials. Each functionality should satisfy the basic requirements of security, privacy, reliability, and ease of use.

In February 2007, FVAP partnered with the DoD's Business Transformation Agency (BTA) to structure a timeframe for the development and release of an electronic voting solution for 2008. The first task was the release of a Request for Information (RFI) to solicit general technological solutions from industry that satisfy three separate absentee voting tasks: electronic voter registration, electronic ballot request, and electronic blank ballot delivery. Solutions needed to support varying state requirements and legally allowed methods of transmittal. The RFI did not indicate any preference of implementation in order to encourage a wide range of methodologies. On March 1, 2007 the RFI was posted on the Federal Business Opportunities website (www.fbo.gov) with a response date of March 30, 2007. The FVAP alerted vendors who had previously expressed an interest in working with the Department of the RFI and directed them to the website. The RFI generated 7 responses, all of which contained some level of applicable technology.

In June of 2007 the FVAP will issue a Request for Proposal (RFP) to solicit specific technological solutions that satisfy the Department's electronic voting requirements. The RFP will be structured to accommodate a multi-phased development plan comprised of a base system and 2 options. These components will be built as individual modules that could be integrated into future expanded services which may include an internet voting system for *UOCAVA* citizens.

The base system provides a voter registration and ballot request solution that is based on the automated FPCA embedded with state-specific requirements which can be completed by the voter and transmitted electronically or via regular mail to local election officials. It will provide local election officials with a transparent, visible and flexible system that allows them to manage the registration and ballot request process according to their state's legal requirements and their available electronic infrastructure. Because voting regulations vary enormously from state to state, the system must provide for a range of information transmission options.

As funding permits, Option 1 will provide a blank ballot delivery system which will be integrated with the Base voter registration/ballot request system. Option 2 will provide for digital signature identity management for both election officials and citizen users. It may accommodate both DoD Common Access Card digital certificates as well as comparable certificates issued by other approved authorities, both governmental and commercial. These digital signatures can serve as the citizen's "wet signature" on the FPCA, and as an initial identifier for system logon.

Any system developed will allow for laboratory and live testing with all potential users throughout the design and implementation period, as well as allowing time for certification and accreditation for all computer and privacy related laws and government guidance. Barring external complications, the following timeline is anticipated:

- June 2007—Release of the RFP
- August 2007—Responses to the RFP will be evaluated and a contract awarded
- December 2007—Base solution availability for implementation in time for primary elections

- March 2008—Option 1 delivery
- June 2008—Option 2 delivery

As each tool becomes available, the FVAP will engage the states by soliciting their input as stakeholders and providing education and training at the state and local election official levels. The FVAP will use national conferences, news releases, teleconferences, letters, and other forums to gather input from, and provide information to the states, voters and the worldwide network of Voting Assistance Officers. Additional capabilities will be considered for 2010 based on lessons learned and evaluation of outcomes of the tools utilized during the 2008 election cycle.