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)

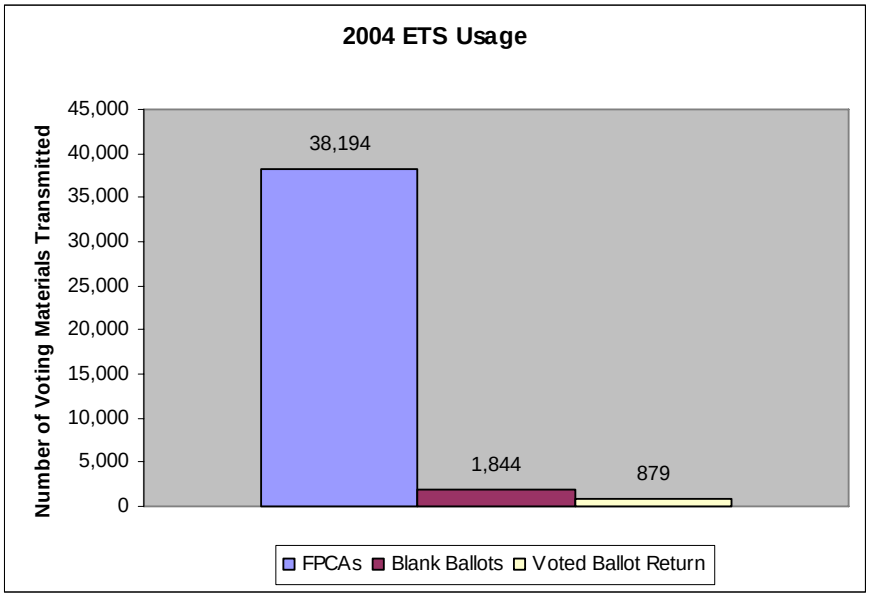
When military personnel were deployed for Operation Desert Shield in 1990, it was not possible to use the normal procedures for absentee voting for all personnel, since round trip transit time for mail delivery of election materials exceeded the time available to vote absentee in the election. In response, 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

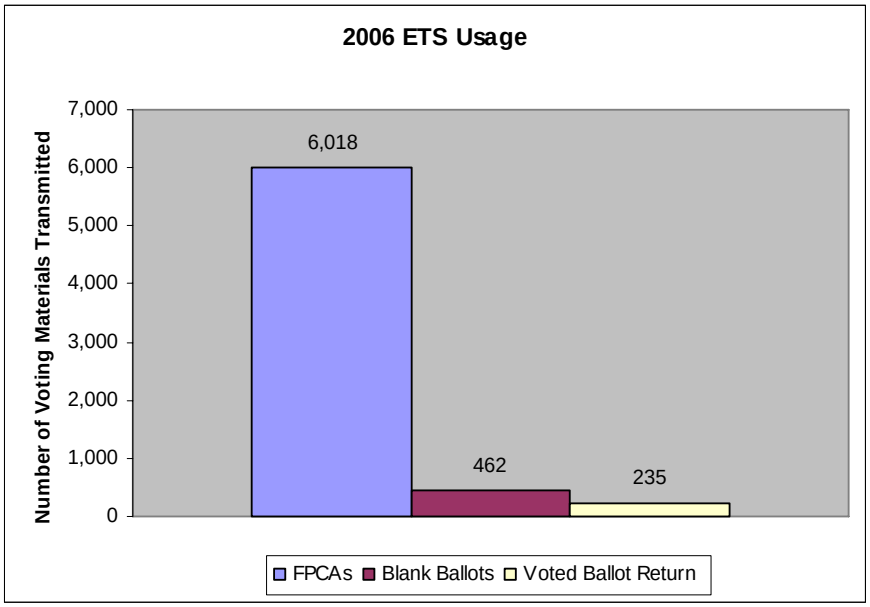
Middle East. The FVAP has continued use of the ETS and many states and territories have legislatively or administratively made changes in their election laws to provide for this method of transmitting election materials for *UOCAVA* citizens.

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.

United States Government Accountability Office

GAO

Report to Congressional Committees

June 2007

ELECTIONS

Action Plans Needed to Fully Address Challenges in Electronic Absentee Voting Initiatives for Military and Overseas Citizens

GAO-07-774

June 2007

ELECTIONS

Action Plans Needed to Fully Address Challenges in Electronic Absentee Voting Initiatives for Military and Overseas Citizens

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-774, a report to congressional committees

Why GAO Did This Study

The Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) protects the rights of military personnel, their dependents, and overseas citizens to vote by absentee ballot. The Department of Defense (DOD) and others have reported that absentee voting, which relies primarily on mail, can be slow and may, in certain circumstances, serve to disenfranchise these voters. In 2004, Congress required DOD to develop an Internet-based absentee voting demonstration project and required the Election Assistance Commission—which reviews election procedures—to develop guidelines for DOD's project. In 2006, Congress required DOD to report, by May 15, 2007, on plans for expanding its use of electronic voting technologies and required GAO to assess efforts by (1) DOD to facilitate electronic absentee voting and (2) the Commission to develop Internet voting guidelines and DOD to develop an Internet-based demonstration project. GAO also assessed DOD's efforts to develop plans to expand its use of electronic voting technologies. GAO interviewed officials and reviewed and analyzed documents related to these efforts.

What GAO Recommends

GAO made recommendations to DOD regarding security, guidance, and plans for electronic voting initiatives and to the Commission on plans to develop the guidelines. DOD and the Commission agreed with these recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-774.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Derek Stewart at (202) 512-5559 or stewartd@gao.gov.

What GAO Found

Since 2000, DOD has developed several initiatives to facilitate absentee voting by electronic means such as fax or e-mail; however, some of these initiatives exhibited weaknesses or had low participation rates that might hinder their effectiveness. For example, the 2003 Electronic Transmission Service's fax to e-mail conversion feature allows UOCAVA voters who do not have access to a fax machine to request ballots by e-mail and then converts the e-mails to faxes to send to local election officials. DOD officials told us, however, they have not performed, among other things, certification tests and thus are not in compliance with information security requirements. The 2004 Interim Voting Assistance System (IVAS)—which, DOD reported, enabled UOCAVA voters to *request* and *receive* ballots securely—cost $576,000, and 17 citizens received ballots through it. The 2006 Integrated Voting Alternative Site (also called IVAS)—which enabled voters to *request* ballots using one tool, by mail, fax, or unsecured e-mail—raised concerns, from Congress and others, that using unsecured e-mail could expose voters to identity theft if they transmit personal data. While this IVAS displayed a warning that voters had to read to proceed, it did not advise them to delete personal voting information from the computers they used. DOD spent $1.1 million, and at least eight voted ballots were linked to this 2006 IVAS. Both the 2004 and 2006 IVAS were each implemented just 2 months before an election. DOD also has a Web site with links to guidance on electronic transmission options, but some of this guidance was inconsistent and could be misleading. DOD officials acknowledged the discrepancies and addressed them during GAO's review.

The Election Assistance Commission has not developed the Internet absentee voting guidelines for DOD's use, and thus DOD has not proceeded with its Internet-based absentee voting demonstration project. Commission officials told GAO that they had not developed the guidelines because they had been devoting constrained resources to other priorities, including challenges associated with electronic voting machines. Furthermore, they have not established—in conjunction with major stakeholders like DOD—tasks, milestones, and time frames for completing the guidelines. The absence of such guidelines has hindered DOD's development of its Internet-based demonstration project. To assist the Commission, however, DOD has shared information on the challenges it faced in implementing prior Internet projects—including security threats.

GAO observed that DOD was developing, but had not yet completed, plans for expanding the future use of electronic voting technologies. Because electronic voting in federal elections involves numerous federal, state, and local-level stakeholders; emerging technology; and time to establish the initiatives, developing results-oriented plans that identify goals, time frames, and tasks—including addressing security issues—is key. Without such plans, DOD is not in a position to address congressional expectations to establish secure and private electronic and Internet-based voting initiatives.

Contents

Tables

Figures

Abbreviations

DOD	Department of Defense
FVAP	Federal Voting Assistance Program
HTML	Hypertext Markup Language
IVAS	Interim Voting Assistance System
IVAS	Integrated Voting Alternative Site
NDAA	National Defense Authorization Act
OMB	Office of Management and Budget
PDF	Portable Document Format
SERVE	Secure Electronic Registration and Voting Experiment
UOCAVA	Uniformed and Overseas Citizens Absentee Voting Act
VAG	Voting Assistance Guide

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

June 14, 2007

The Honorable Carl Levin
Chairman
The Honorable John McCain
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Ike Skelton
Chairman
The Honorable Duncan Hunter
Ranking Member
Committee on Armed Services
House of Representatives

A citizen's right to vote is one of the hallmarks of a democratic society; yet exercising this right can be a challenge for millions of military personnel and their dependents of voting age who live away from their legal residences (in or outside the United States) and for overseas citizens. These individuals are eligible to vote by absentee ballots in federal elections. This eligibility is established by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA),[1] which is administered by the Department of Defense's (DOD) Federal Voting Assistance Program (FVAP). Through this program, DOD provides assistance to UOCAVA voters to facilitate opportunities for them to exercise their right to vote. The absentee voting process requires the potential voter to register to vote, request an absentee ballot, receive the ballot, correctly complete the ballot, and return it to the appropriate local election official. However, DOD and groups that represent voters covered under the act have reported that, because the multistep process of absentee voting relies primarily on mail, in some instances it can take so long to complete that these voters may, in effect, be disenfranchised.

[1]Pub. L. No. 99-410 (1986), 42 U.S.C. §§ 1973ff et seq.

To address concerns about mail-based absentee voting, Congress has enacted several laws to promote electronic means for voters to register, request and receive ballots, and transmit voted ballots to local election officials. These laws include (1) the Help America Vote Act of 2002, which established the Election Assistance Commission to serve as a national clearinghouse for election information and to review election procedures; develop voluntary voting system guidelines;[2] and study, among other things, electronic voting—particularly Internet voting technology; (2) section 1604 of the National Defense Authorization Act (NDAA) for Fiscal Year 2002, which required DOD to carry out a secure[3] Internet-based electronic demonstration project[4] in the general election for federal office in 2002 or 2004; and (3) section 567 of the Ronald W. Reagan NDAA for Fiscal Year 2005, which amended Congress's mandate for DOD to develop a secure, Internet-based, absentee voting demonstration project—by requiring DOD to implement the project during the first general election for federal office that occurs after the Election Assistance Commission establishes Internet voting guidelines for the absentee voting process.[5] Section 596 of the John Warner NDAA for Fiscal Year 2007 required DOD to submit, not later than May 15, 2007, a detailed plan to expand the use of electronic voting technology.

Section 596 of the John Warner NDAA for Fiscal Year 2007 also required GAO to review DOD's electronic and Internet-based voting initiatives. This report assesses (1) DOD's efforts to facilitate registration, ballot

[2]Voluntary voting system guidelines are to provide a set of specifications and requirements to be used in the certification of computer-assisted voting systems, both paper-based and fully electronic; states are free to adopt these guidelines in whole or in part or reject them entirely.

[3]In 1998, DOD had voluntarily initiated a proof of concept called "Voting Over the Internet," which was a small-scale Internet-based project used in the 2000 elections. DOD's report on this proof of concept acknowledged that a larger-scale pilot would result in more visibility and potentially attract those with malicious intent to harm the system, but suggested ways to mitigate such future attacks. To address these security concerns and other issues, Congress asked DOD, in 2002, to develop a large-scale, Internet-based demonstration project to ensure a methodical progression from the current mail-based process to a secure, easy-to-use Internet registration and voting system.

[4]One of the primary objectives of the electronic demonstration project was to assess the use of such technologies to improve UOCAVA participation in elections.

[5]The conference report for the bill noted that DOD's prototype for electronic voting was important and should not be abandoned and encouraged the Secretary of Defense to provide funding to the Commission to advance electronic absentee voting by UOCAVA voters. H.R. Rep. No. 108-767, at 680 (2004) (Conf. Rep.).

transmittal, and voting by electronic means, such as e-mail and fax, for UOCAVA voters and (2) the Election Assistance Commission's efforts to develop Internet absentee voting guidelines and DOD's efforts to develop a secure, Internet-based, absentee voting demonstration project. The report also discusses DOD's efforts to develop plans to expand the use of electronic voting technology in the future.

To address our objectives, we reviewed and analyzed laws, directives, reports, and plans related to DOD's efforts to provide electronic voting capabilities for UOCAVA voters. We also examined the Election Assistance Commission's efforts to develop Internet absentee voting guidelines. We reviewed and analyzed information regarding any benefits and challenges that we, DOD, and others had identified related to DOD's Internet-based electronic demonstration project and new electronic voting initiatives, along with the steps DOD had taken to mitigate those challenges. Additionally, we interviewed and obtained documentation from officials in several offices within DOD, the Election Assistance Commission, selected state and local election jurisdictions, and some independent groups concerned with the interests of UOCAVA voters. We performed our work in accordance with generally accepted government auditing standards, from August 2006 through April 2007. Appendix I provides detailed information about our scope and methodology.

Results in Brief

Since the 2000 federal election, DOD has developed several initiatives to facilitate voting by electronic means such as fax or e-mail; however, some of these initiatives exhibited weaknesses or garnered low participation rates that could limit their effectiveness. DOD introduced the first of three initiatives, an e-mail to fax conversion enhancement to its Electronic Transmission Service, in 2003. This feature allows UOCAVA voters who do not have access to a facsimile machine to send ballot requests, via e-mail, to DOD's Electronic Transmission Service, which converts e-mail messages to faxes and sends them to local election officials.[6] In return, local election officials can send ballots to the Electronic Transmission Service conversion feature by fax; the conversion feature then converts the fax to an e-mail and sends it to the voter. DOD officials told us, however, that this feature is not in compliance with certain DOD

[6]The Federal Voting Assistance Program reported that some states, by law, allow voting materials to be sent by fax but not by e-mail.

information security requirements,[7] which include performing and documenting risk assessments and security certification testing. Without such compliance, DOD cannot certify that it has employed the basic practices necessary to apply security measures. DOD officials said that they plan to award a contract to meet the requirements. Also, DOD voluntarily launched a second initiative—the Interim Voting Assistance System (IVAS)—in September 2004, to enable, as DOD reported, absentee voters to request and receive state or territory ballots securely for use in the November 2004 election. DOD spent $576,000 on this project, but only 17 citizens received ballots through this system—in part, because it was implemented just 2 months before the election. Further, in September 2006, DOD developed, in response to a legislative mandate,[8] a third initiative—the Integrated Voting Alternative Site (also called IVAS). This site included (1) a ballot *request* only tool—called Tool 1—that enabled voters to request their state or territory ballots from election officials by fax, regular mail, or unsecured e-mail and (2) a ballot *request* and *receipt* tool—called Tool 2—that enabled voters to request and receive their state or territory ballots through a secured server. Officials within Congress, and others, expressed concerns that using the Tool 1 with unsecured e-mail could expose voters to the risk of identity theft. DOD displayed a warning on the site—which voters had to read to continue processing their request—that explained the risks associated with e-mailing ballot requests. While the warning addressed the risks of transmitting personal identification information by e-mail, it did not inform voters of the risks involved in leaving such personal information on the computers they used—especially public computers or those shared by others. DOD officials said they would incorporate lessons learned, such as adding a cautionary statement to future systems to warn UOCAVA voters to remove personal information from the computers they use. DOD spent about $1.1 million on the 2006 IVAS, but local election officials could link only eight ballots to IVAS Tool 2.[9] In addition to these initiatives, DOD has established a Web site with links to guidance that provides UOCAVA

[7]DOD, *Interim Department of Defense (DOD) Certification and Accreditation (C&A) Process Guidance*, July 6, 2006.

[8]Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Hurricane Recovery, 2006. Pub. L. No. 109-234 (2006).

[9]FVAP reported that, since ballot requests could be printed and returned through the mail or by fax instead of the secured server, an accurate reporting could not be obtained through Tool 2. FVAP also reported that ballot requests submitted using Tool 1 could not be tracked and reported because voters sent the requests directly to local election officials using their personal e-mail accounts, mail, or fax.

voters with, among other things, information on electronic alternatives to mail for each of the 55 states and territories. These links lead to DOD's 2006 IVAS, the Voting Assistance Guide, news releases, and guidance updates. Our analysis of information on DOD's Web site, however, showed that for 14 of the 55 states and territories, some of the information about the alternatives was inconsistent and could be misleading. For example, for one state, information on three links correctly stated that only overseas military and overseas civilian voters were eligible to receive or return a ballot by fax; however, a fourth link did not include this restriction. As a result, military personnel stationed in the United States, but away from their state of residence, may have incorrectly concluded that they were eligible to vote by fax. While these inconsistencies were not widespread, their mere existence could lead UOCAVA voters to rely on incorrect information and therefore adversely affect the citizens' ability to vote. Agency officials acknowledged these discrepancies and addressed them during the course of our review. We are recommending that DOD improve the security and accuracy of its systems by (1) complying with information security requirements, (2) incorporating lessons learned, such as adding a cautionary statement to future systems to warn UOCAVA voters to remove personal information from the computers they use, and (3) institutionalizing a review process for its online guidance to ensure that information for absentee voters is accurate and consistent. DOD concurred with these recommendations.

The Election Assistance Commission has not yet developed guidelines for Internet absentee voting for DOD's use, and, thus, DOD has not proceeded with developing its secure, Internet-based, absentee voting demonstration project. Specifically, Commission officials stated that they had not yet developed the guidelines because they had been devoting constrained resources to meeting the challenges associated with current electronic voting machines. Furthermore, the Commission has not yet established—in conjunction with major stakeholders, like DOD—tasks, including addressing security and privacy risks; time frames; or milestones for completing the guidelines. Similarly, DOD has not developed the secure, Internet-based, absentee voting demonstration project because, DOD officials said, by law, the Commission must develop Internet absentee voting guidelines for DOD to follow before it can proceed. To support the Commission in developing these guidelines, DOD officials said they gave the Commission a report and an internal DOD document that provides the framework for a system, along with challenges DOD found in its earlier Internet voting projects. These challenges included security threats such as computer viruses, malicious insider attacks, and inadvertent errors that could disrupt system performance. DOD officials stated that, even if the

Internet absentee voting guidelines had been available at the time of our review, the time remaining before the 2008 federal election would be inadequate for developing the secure, Internet-based, demonstration project. We are recommending that the Election Assistance Commission, in conjunction with major stakeholders such as DOD, create an action plan with tasks including actions to address the security and privacy risks associated with Internet voting processes and time frames for developing the Internet absentee voting guidelines. The Election Assistance Commission concurred with our recommendation.

We observed that DOD was developing, but had not yet completed, plans for expanding the use of electronic voting technology for military personnel and overseas citizens, as required by the John Warner NDAA for Fiscal Year 2007. The act requires DOD to submit these plans to Congress, not later than May 15, 2007. Our analysis of existing DOD and Commission documents and our interviews with agency officials show that DOD has not sufficiently involved stakeholders in recent electronic voting efforts—such as its 2006 IVAS. In addition, it has not established interim tasks that address issues such as security and privacy, milestones, time frames, or contingency plans, following the sound management practices used by leading organizations. Implementation of new electronic voting initiatives requires careful planning, particularly in light of the large number of stakeholders, the application of new technology, the remote location of troops, and the lead time required for implementation. Without an integrated, results-oriented plan that involves all stakeholders and identifies, among other things, goals, tasks, time frames, and contingency plans, DOD is not in a position to address congressional expectations to establish secure and private electronic and Internet-based voting initiatives. We are recommending that DOD, in conjunction with major stakeholders such as the Election Assistance Commission and local election officials, develop a comprehensive, results-oriented plan for future efforts that specifies, among other things, tasks including identifying safeguards for security and privacy of all DOD's voting systems—both electronic and Internet-based. DOD concurred with this recommendation.

DOD's and the Commission's written comments are contained in appendixes III and IV, respectively. DOD also provided technical comments, which we incorporated in the final report, as appropriate.

Background

The U.S. election system is highly decentralized and relies on a complex interaction of people, processes, and technology. Voters, local election

jurisdictions (which number over 10,000), states and territories, and the federal government all play important roles in the election process. The process, however, is primarily the responsibility of the individual states and territories and their election jurisdictions. As we reported in our 2006 testimony,[10] states and territories have considerable discretion in how they organize the elections process; this is reflected in the diversity of procedures and deadlines that states and jurisdictions establish for voter registration and absentee voting. Furthermore, these states and jurisdictions use a variety of voting techniques, from paper ballots to faxes and e-mails. We also reported that the voter is ultimately responsible for being aware of and understanding the absentee voting process and taking the actions necessary to participate in it.

The UOCAVA established that members of the military and their dependents of voting age living away from their legal residences (in or outside the United States) and American citizens who no longer maintain a permanent residence in the United States are eligible to participate by absentee ballot in all federal elections. According to DOD, the act covers more than 6 million people. Executive Order and DOD guidance related to the act include the following:

- Executive Order 12642, dated June 8, 1988, made the Secretary of Defense, or his designee, responsible for carrying out the federal functions under UOCAVA, including (1) compiling and distributing information on state absentee voting procedures, (2) designing absentee registration and voting materials, (3) working with state and local election officials, and (4) reporting to Congress and the President after each presidential election on the effectiveness of the program's activities (including a statistical analysis of UOCAVA voters' participation).

- DOD Directive 1000.4, updated April 14, 2004, assigned the Office of the Under Secretary of Defense for Personnel and Readiness responsibility for administering and overseeing the program, and it established the FVAP to manage the program. In 2006, FVAP officials told us that they were authorized a full-time staff of 13 and had a fiscal year budget of approximately $3.8 million.

FVAP facilitates the absentee voting process for UOCAVA voters; its mission is to (1) inform and educate U.S. citizens worldwide about their

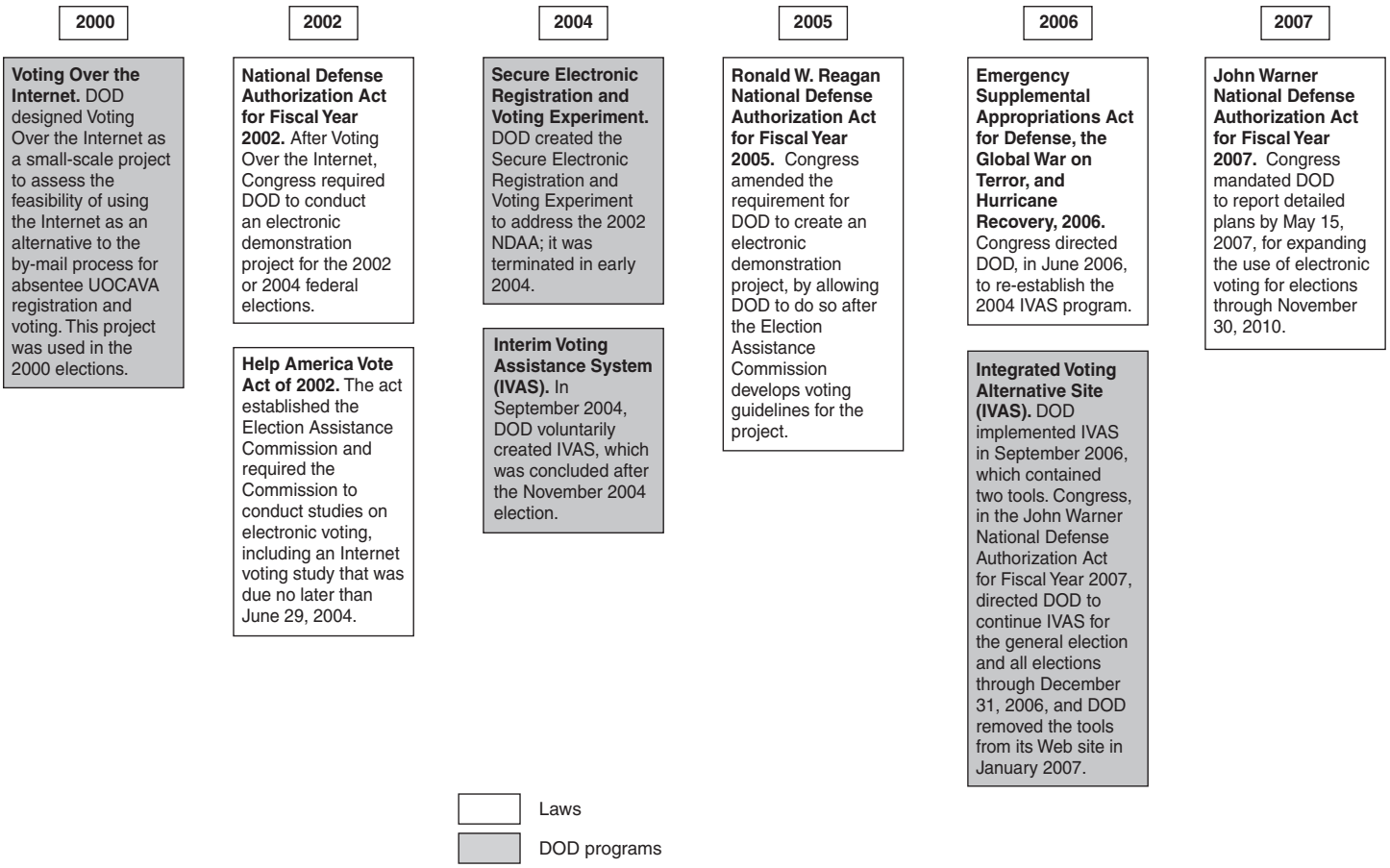
[10]GAO, *Elections: DOD Expands Voting Assistance to Military Absentee Voters, but Challenges Remain*, GAO-06-1134T (Washington, D.C.: Sept. 28, 2006).

right to vote, (2) foster voter participation, and (3) enhance and protect the integrity of the electoral process at the federal, state, and local levels. FVAP also, among other things, provides training opportunities for Voting Assistance Officers (service, State Department, and overseas citizen organization officials who carry out the implementation of their respective voting assistance programs); prescribes, coordinates, and distributes voting materials, such as the Federal Post Card Application (the registration and absentee ballot request form for UOCAVA voters); and provides for alternatives to regular mail, including Express Mail and the use of electronic solutions.

The Election Assistance Commission, which was established by the Help America Vote Act of 2002, also contributes to the absentee voting process. The act specifically established the Commission as a national clearinghouse for election information and procedures and assigned it responsibility for developing voting system guidelines for the entire election process. The act also specifies that the development of voluntary voting system guidelines should be informed by research and development in remote access voting, including voting through the Internet, and the security of computers, networks and data storage. In 2005, the Commission issued guidelines that, among other things, addressed gaps in the security measures of prior standards. However, these guidelines do not comprehensively address telecommunications and networking services or their related security weaknesses, such as those related to the Internet. The act also amended UOCAVA to require states to report to the Commission, after each regularly scheduled general election for federal office, on the aggregate number of (1) absentee ballots transmitted to absentee uniformed services voters and overseas voters for the election and (2) ballots returned by those voters and cast in the election. The Commission collects this information through its biennial state surveys of election data.

DOD, the Commission, and organizations representing UOCAVA voters have noted that these voters may effectively become disenfranchised because the multistep process for voting by absentee ballot—which relies primarily on mail—can take too long, especially for mobile servicemembers and overseas citizens or those deployed to or living in remote areas. Congress and DOD have taken action to facilitate the use of alternatives to mail, including electronic means such as fax, e-mail, and the Internet. Figure 1 shows (1) the laws designed to facilitate the use of electronic capabilities for UOCAVA voters and (2) some of DOD's efforts, either voluntary or in response to a statute, to provide electronic capabilities to these voters during fiscal years 2000 through 2007.

Figure 1: Laws and Some DOD Programs Promoting Electronic Alternatives to Mail for UOCAVA Voters, 2000 through 2007



Source: GAO analysis of Laws and DOD information.

FVAP stated that it implemented the Voting Over the Internet project in 2000 as a small-scale pilot project to provide military personnel and their dependents and overseas citizens covered under UOCAVA the ability to securely register to vote, request and receive ballots from local election officials, and vote via the Internet. DOD voluntarily developed the project as a small-scale proof-of-concept Internet voting project. This project enabled 84 voters to vote over the Internet—the first time that binding votes were cast in this manner.[11] While the project demonstrated that it

[11]UOCAVA voters in Florida, South Carolina, Texas, and Utah, who were away from their legal residences, cast a total of 84 votes from their homes, workplaces, or duty stations on personal computers.

was possible for a limited number of voters to cast ballots online, DOD's report concluded that security concerns needed to be addressed before it could expand remote (i.e., Internet) voting to a larger population.

In 2001, Congress noted that the Voting Over the Internet project had demonstrated that the Internet could be used to enhance absentee voting.[12] To continue the examination of a secure, easy-to-use Internet voting system as an alternative to the regular mail process, Congress mandated, in the NDAA for Fiscal Year 2002, that DOD conduct a large-scale Internet-based absentee voting demonstration project to be used for the 2002 or 2004 federal election. DOD responded to this mandate by creating the Secure Electronic Registration and Voting Experiment (SERVE) for Internet-based absentee registration and voting; SERVE used a system architecture similar to the one used for the Voting Over the Internet project. However, as we previously reported,[13] a minority report published by four members of the Security Peer Review Group—a group of 10 computer election security experts that FVAP assembled to evaluate SERVE—publicly raised concerns about the security of the system because of its use of the Internet.[14] The four members suggested that SERVE be terminated because potential security problems left the information in the system vulnerable to cyber attacks that could disclose votes or personal voter information. Furthermore, they cautioned against the development of future electronic voting systems until the security of both the Internet and the world's home computer infrastructure had been improved. Because DOD did not want to call into question the integrity of votes that would have been cast via SERVE, the Deputy Secretary of Defense terminated the project in early 2004, and DOD did not use it in the November 2004 election.

[12]The U.S. Senate Committee on Armed Services report on Senate bill 1416 regarding the NDAA for Fiscal Year 2002 noted that the Voting Over the Internet project was an important first step in assessing how to use the Internet to enhance absentee voting; reducing traditional barriers to participation in elections by absentee voters; and providing insight into issues that must be considered for broader use of remote registration and voting through the Internet. (S. Rep. No. 107-62, at 307 [2001]).

[13]GAO, *Elections: Absentee Voting Assistance to Military and Overseas Citizens Increased for the 2004 General Election, but Challenges Remain*, GAO-06-521 (Washington, D.C.: Apr. 7, 2006).

[14]Security Peer Review Group, *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*, January 21, 2004. The Security Peer Review Group consisted of 10 experts on computer security and voting systems drawn from academia and the private sector. As stated above, the report was written by 4 of the 10 experts.

The points raised in these security reviews are consistent with concerns we raised in our 2001 reports.[15] We found that broad application of Internet voting presented formidable social and technological challenges. In particular, we noted that challenges to remote Internet voting[16] involve securing voter identification information and ensuring that voters secure the computer on which they vote. We also reported that because voting requires more stringent controls than other electronic transactions, such as online banking, Internet voting systems face greater security challenges than other Internet systems. Furthermore, we found that remote Internet voting was recognized as the least protective of ballot secrecy[17] and voter privacy[18] and was most at risk from denial of service and malicious software, such as computer viruses. While opinions of groups considering the pros and cons of Internet voting were not unanimous, we found that they agreed in principle on major issues, including considering security to be the primary technical challenge for Internet voting.[19] Because of serious concerns about protecting the security and privacy of the voted ballot, we concluded that Internet-based registration and voting would not likely be implemented on a large scale in the near future.

In the Ronald W. Reagan NDAA for Fiscal Year 2005, Congress amended the requirement for the Internet-based absentee voting demonstration project by permitting DOD to delay its implementation until the first federal election after the Election Assistance Commission developed guidelines for the project. The conference report for the act[20] stated that,

[15]GAO, *Elections*: *Voting Assistance to Military and Overseas Citizens Should be Improved*, GAO-01-1026 (Washington, D.C.: Sept. 28, 2001) and *Elections*: *Perspectives on Activities and Challenges Across the Nation*, GAO-02-3 (Washington, D.C.: Oct. 15, 2001).

[16]Various approaches to Internet voting are possible, ranging from the use of Internet connections at traditional polling stations to the ability to remotely vote from anywhere (remote Internet voting). An intermediate step along this range is an option referred to as "kiosk voting," which uses conveniently located voting terminals provided and controlled by election officials.

[17]Ballot secrecy refers to protecting the content of the vote.

[18]Voter privacy refers to protecting the voters' ability to cast votes without being observed. In poll-site voting, voter privacy is generally ensured by election officials and observers. However, we reported that remote Internet voting would not protect voters' physical privacy, leaving them open to the risk that they might be coerced (through threats, bribery, or other forms of pressure).

[19]Other challenges that affect implementation of Internet voting include the costs of the voting method versus its benefits and the availability of Internet technology to voters.

[20]H.R. Rep No. 108-767, at 680 (2004) (Conf. Rep.).

although Congress recognized the technical challenges of Internet voting, SERVE was an important prototype that should not be abandoned.

DOD Initiatives Assist UOCAVA Voters, but Certain Weaknesses May Limit Their Effectiveness

Since the 2000 federal election, DOD has established several initiatives as alternatives to the by-mail process to facilitate voter registration and ballot request, receipt of a ballot, and submission of a voted ballot by electronic means—such as fax and e-mail—for UOCAVA voters. These include the Electronic Transmission Service's fax to e-mail and e-mail to fax conversion enhancement (hereafter referred to as the e-mail to fax conversion feature); the 2004 Interim Voting Assistance System (IVAS); the 2006 Integrated Voting Alternative Site (also called IVAS); DOD's online voting assistance guidance; and online forms to register, request, receive, or submit ballots. While these efforts provide valuable guidance, services, and information to UOCAVA voters, some of them had limited participation rates or exhibited weaknesses in security, consistency, and accuracy that might hinder their use and effectiveness. DOD officials have acknowledged these weaknesses and they began taking action to address them during the course of our review.

Electronic Transmission Service's E-mail to Fax Conversion Capability Facilitates Transmission of Voting Materials but Does Not Fully Comply with Information Security Requirements

The electronic transmission service is a fax forwarding system, established by FVAP in 1990, that allows UOCAVA voters and state and local election officials, where permitted by law, to fax election materials to each other. These voters and election officials can use this service and do not have to pay long distance fees for faxing out of state, because DOD provides the service through a toll-free line. In 2003, after discussions with Mississippi state officials and a Mississippi National Guard unit, FVAP added the e-mail to fax conversion capability to its electronic transmission service. These officials asked FVAP for help in transmitting voting materials because, by state law, Mississippi allowed only faxing as an electronic means of transmission—a capability that the Guard unit would not have while it was deployed to Iraq.[21] The e-mail to fax conversion feature allows UOCAVA voters who do not have access to a facsimile machine to send ballot requests, via e-mail, to DOD's Electronic Transmission Service, which converts e-mail attachments to faxes and sends them to local election officials. In return, local election officials can send ballots to the Electronic Transmission Service conversion feature by fax; the conversion

[21]The FVAP reported that some states, by law, allow voting materials to be sent by fax but not by e-mail.

feature then converts the fax to an e-mail attachment and sends it to the voter.

FVAP stated that it notifies states and territories whenever it converts an e-mail containing voting materials to a fax, or vice versa, so that the state or territory can decide whether or not to accept it. Table 1 shows Electronic Transmission Service activity for the conversion feature for 2004 and 2006.

Table 1: Electronic Transmission Service E-mail to Fax Conversions for 2004 and 2006

	Years	
	2004	**2006**
E-mails converted to fax—sent from citizens to local election officials		
Voted ballots	67	53
Federal post card applications and remaining ballot materials	389	190
Subtotal	**456**	**243**
E-mails converted to fax—sent from local election officials to citizens[a]		
Federal post card applications and remaining ballot materials	153[b]	182
Subtotal	**153[b]**	**182**
Total	**609**	**425**

Source: DOD.

[a]FVAP officials stated that the local election officials who send e-mails to the Electronic Transmission Service conversion feature use it to store ballots that will be sent to UOCAVA voters, through DOD, at some future date.

[b]FVAP noted that for the 2004 elections the Electronic Transmission Service conversion feature received 61 e-mails from local election officials which they converted to 153 faxes to citizens covered under UOCAVA. FVAP explained that this allowed one local election official to send one e-mail with a PDF attachment to the Electronic Transmission Service, which would then get converted to a fax and sent to multiple UOCAVA voters per the local election official's instructions. PDF means Portable Document Format; it is a file format that is used to view electronic copies of paper documents, which allows an exact copy of the paper document.

Although FVAP has made progress in assisting servicemembers to transmit voting materials with the e-mail to fax conversion enhancement, FVAP officials told us they have not fully complied with certain information security requirements in the Interim DOD Information Assurance Certification and Accreditation Process.[22] This guidance

[22]DOD, *Interim Department of Defense (DOD) Certification and Accreditation (C&A) Process Guidance*, July 6, 2006.

requires DOD components, among other things, to implement controls and to certify and accredit such e-mail systems.

FVAP officials initially stated that the information security guidance did not apply to the conversion feature; they saw it as an enhancement to the original Electronic Transmission Service's fax system. During the course of our review, however, FVAP officials said they consulted with officials responsible for DOD's information assurance certification and accreditation and concluded that the requirements did, in fact, apply. These officials stated that, by the end of fiscal year 2007, they plan to award a contract to obtain services to meet the information security requirements. The FVAP officials further stated that, while they do not have the required documentation—such as risk assessments or certification tests and accreditations—they have taken some measures to ensure security. We note that the statement of work for FVAP's April 29, 2005, contract for the Electronic Transmission Service recognizes the sensitivity of the data associated with election materials and includes provisions for certain security functions, such as ensuring that adequate steps are taken to prevent unauthorized access or manipulation of the data. Until FVAP performs and documents the security assessments and certifications, however, it has not taken all the necessary measures to secure its system and comply with DOD's information security requirements.

Federal law includes a number of separate statutes that provide privacy protections for certain information. The major requirements for the protection of personal privacy by federal agencies come from two laws: the Privacy Act of 1974[23] and the privacy provisions of the E-Government Act of 2002. Section 208 of the E-Government Act of 2002[24] requires agencies, among other things, to conduct privacy impact assessments before developing, upgrading, or procuring information technology that collects, maintains, or disseminates personally identifiable information. DOD developed departmentwide guidance—the DOD Privacy Impact Assessment Guidance—for implementing the privacy impact assessment requirements mandated in the E-Government Act of 2002. In this guidance, DOD directs the components to adhere to the requirements prescribed by the Office of Management and Budget (OMB)—Guidance for

[23]5 U.S.C. § 552a.

[24]Pub. L. No. 107-347 (2002).

Implementing the Privacy Provisions of the E-Government Act of 2002.[25] FVAP officials stated that they had not conducted a privacy impact assessment for the Electronic Transmission Service's e-mail to fax conversion enhancement, but they told us that a privacy impact assessment will be done as part of the previously mentioned contract to meet information security requirements. A privacy impact assessment would identify specific privacy risks to help determine what controls are needed to mitigate those risks associated with the Electronic Transmission Service. Furthermore, building in controls to mitigate risks could ensure that personal information that is transmitted is only used for a specified purpose. FVAP noted that when information is sent by e-mail, the conversion feature retains the following information: full name, fax number, city, state, zip code, and e-mail addresses. FVAP's Electronic Transmission Service retains this personally identifiable information both to provide transmission verification or confirmation to users and to comply with election document retention requirements under the Civil Rights Act of 1960.[26]

DOD's Electronic Ballot Request and Receipt Initiatives Had Limitations in Participation and Security

In September 2004, just 2 months prior to the election, DOD voluntarily implemented what it reported as a secure electronic system for voters to *request* and *receive* ballots—the Interim Voting Assistance System (IVAS)—as an alternative to the traditional mail process. IVAS was open to active duty servicemembers, their voting age dependents, and DOD overseas personnel who were registered in a state or territory participating in the project[27] and enrolled in the Defense Enrollment Eligibility Reporting System—a DOD-managed database that includes over 23 million records pertaining to active duty and reserve military and their family members, retired military, DOD civil service personnel, and DOD contractors. DOD had limited IVAS participation to UOCAVA voters who were affiliated with DOD because their identities could be verified in the Defense Enrollment Eligibility Reporting System. Voters obtained their state or territory ballots through IVAS by logging on to a special Web site

[25]OMB, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003. (M-03-22).

[26]Every officer of election must retain and preserve all election records and papers for certain federal elections for a period of 22 months from the date of the election. Civil Rights Act of 1960, § 301, 42 U.S.C. § 1974.

[27]States and territories participating in the 2004 IVAS included Kansas, Kentucky, Maryland, Mississippi, Montana, New Mexico, South Carolina, the Virgin Islands, and Wisconsin.

and then requesting ballots from their participating local election jurisdictions. After the local election officials approved the requests and the ballots were finalized, IVAS notified voters via e-mail that the ballots were available to download and print. DOD reported that 108 counties in eight states and one territory agreed to participate in this 2004 IVAS; however, only 17 citizens downloaded their ballots from the site during the 2004 election. FVAP officials noted that participation was low, in part because this IVAS was implemented just 2 months before the election. FVAP further reported that many states did not participate—for a variety of reasons, including state legislative restrictions, workload surrounding regular election responsibilities, and lack of Internet access. FVAP officials noted that this system, which was maintained through the conclusion of the election, cost $576,000.

In September 2006—again, just 2 months before the next general election—FVAP launched a follow-on Integrated Voting Alternative Site, also called IVAS, in response to a June 2006 legislative mandate to reestablish the 2004 IVAS. This 2006 IVAS expanded on the 2004 effort, by providing information on electronic ballot request and receipt options for all UOCAVA citizens in all 55 states and territories. It also provided two tools that registered voters could access through the FVAP Web site, using DOD or military identification, to request or receive ballots from local election officials. As with the 2004 IVAS, local election officials used information in these tools to verify the identity of UOCAVA voters who used them.[28] The first tool—called Tool 1—contained a ballot *request* form only, accessed through DOD's Web site, which voters could fill out and download to their computers. Voters could then send the downloaded form to the local election officials either by regular mail, fax, or unsecured e-mail, per state or territory requirements. FVAP officials reported to Congress that no information on the number of users was available on the use of Tool 1 because the department was no longer involved in the process once the voter downloaded the ballot request and they, essentially, had no visibility into what transpired directly between the voter and the election officials.

[28]Verification was made by the use of WebGuard, which determines the status of an individual enrolled in the Defense Manpower Data Center's Defense Enrollment Eligibility Reporting System database using that individual's name, Social Security number, and date of birth. Ballot requests saved and downloaded to the voter's computer for voters who used Tool 1 and those requests sent to the election officials using Tool 2 both include text indicating the forms were generated via IVAS.

The second tool—called Tool 2—provided a ballot *request* and *receipt* capability for voters, similar to the 2004 IVAS, which also allowed voters to fill out ballot request forms online, send them to local election officials through a secure line, and receive their state or territory ballots from the local election officials through a secured server. Again, no voted ballots were transmitted through this IVAS system given that it was not designed for that purpose. Absentee voters, instead, would return voted ballots, outside of IVAS, in accordance with state law. Tool 2 had a tracking feature which showed that 63 voters had requested ballots through the system. Of these, local election officials approved and made their state or territory ballots available to 35 UOCAVA voters. However, of the 35 sent out, local election officials reported that only 8 voted ballots[29] were traced back to the IVAS Tool 2, in part because this IVAS was implemented just 2 months before the election. DOD reported that the total cost for the 2006 IVAS was about $1.1 million, and given that the tools were used only to request or receive ballots for the November 2006 elections,[30] DOD removed the tools from FVAP's Web site in January 2007. Table 2 compares and provides additional details on the two tools.

[29]FVAP reported that, since ballot requests could be printed and returned through the mail or by fax instead of the secured server, an accurate reporting could not be obtained through Tool 2. FVAP also reported that ballot requests submitted using Tool 1 could not be tracked and reported because voters sent the requests directly to local election officials using their personal e-mail accounts, mail, or fax.

[30]Congress directed DOD, in June 2006, to reestablish the 2004 IVAS program. Congress also directed, in October 2006, that DOD continue IVAS for the general election and all elections through December 31, 2006.

Table 2: Comparison of Integrated Voting Alternative Site Tools 1 and 2 for Election Year 2006

	Tool 1	Tool 2
Developer/ contractor	Defense Manpower Data Center	Merlin International, Incorporated's PostX
User(s)	• Uniformed servicemembers • Servicemembers' dependents • Overseas DOD employees and contractors	• Uniformed servicemembers • Servicemembers' dependents • Overseas DOD employees and contractors • Local election officials
Tracking	• System is not able to track ballot request forms sent to local election officials because users submitted their Federal Post Card Applications directly to local election officials using their personal e-mail accounts. • System can provide only how many times it was accessed.	• System is able to track ballot request forms sent to local election officials; local election officials reported that they received 8 voted ballots.[a] • PostX reported 63 ballot requests were submitted to the system; 35 were approved—29 out of 35 blank ballots were viewed by voters on the system.
Step-by-step process	• Registered voters use a unique DOD identifier or credential to log in to the IVAS tool. • Voters complete the automated Federal Post Card Applications, without their signature, to request a ballot. • Voters save the Federal Post Card Applications to their computers as PDF files. • Voters e-mail the Federal Post Card Applications over an unsecured Internet line to local election officials; voters may also fax or mail the Federal Post Card Applications to local election officials—depending on state or territory procedures.	• Registered voters use unique DOD identifier or credential to log in to the IVAS tool. • Voters complete the automated Federal Post Card Applications, without their signature, to request a ballot. • Voters save the Federal Post Card Applications to the secure server and the system sends a notification to the local election officials of completed ballot requests. • Local election officials receive automated e-mails with notification of new ballot requests and log onto the secure server to access the Federal Post Card Applications. • Local election officials approve applications and upload blank ballots onto the secure server. • Voters log onto the secure server and fill out ballots. • Voters print completed ballots. • Voters submit voted ballot directly to local election officials, in accordance with state law. • Local election officials confirm voted ballot receipts. • Voters log on to check confirmation of voted ballot receipts.

Source: DOD information.

[a]FVAP reported that, since ballot requests could be printed and returned through the mail or by fax instead of the secured server, an accurate reporting could not be obtained through Tool 2. FVAP also reported that ballot requests submitted using Tool 1 could not be tracked and reported because voters sent the requests directly to local election officials using their personal e-mail accounts, mail, or fax.

Officials within Congress, and others, have expressed concerns that voters could be exposed to a heightened risk of identity theft if they used Tool 1 to send voting materials that contain personally identifiable information (including Social Security number, date of birth, and address), by unsecured e-mail. FVAP officials acknowledged in their December 2006

report to Congress[31] that Tool 1 was less secure, but said (1) DOD was providing access to a capability that states already provide,[32] (2) most states and territories only required the last four digits of the Social Security number on the ballot requests,[33] and (3) Tool 1 displayed a cautionary statement that voters had to read to go on with the request process; this cautionary statement explained the risk associated with e-mailing ballot requests and that the government assumed no liability if voters did so. While we confirmed a cautionary statement related to the transmission of personal data did exist for Tool 1, it did not advise voters, after submitting their ballot request, to remove voting materials that they have stored on their computers. For example, voters using Internet cafes overseas could have been subject to identity theft if they did not delete their personal information from the computer and a subsequent user gained access to the stored file. FVAP officials acknowledged that users were not advised of the risks of storing personal voting information on their computers, and these officials stated that they will incorporate lessons learned, such as adding a cautionary statement in any future ballot request system.

Online Voting Guidance Is Useful but Some Inconsistencies Exist in the Links

In addition to these initiatives, DOD also has established the FVAP Web site,[34] which contains information on FVAP programs and links to assist UOCAVA voters in the voting process. Specifically, these links access FVAP's online guidance, including several versions of FVAP's biennial Voting Assistance Guide, shown in figure 2.

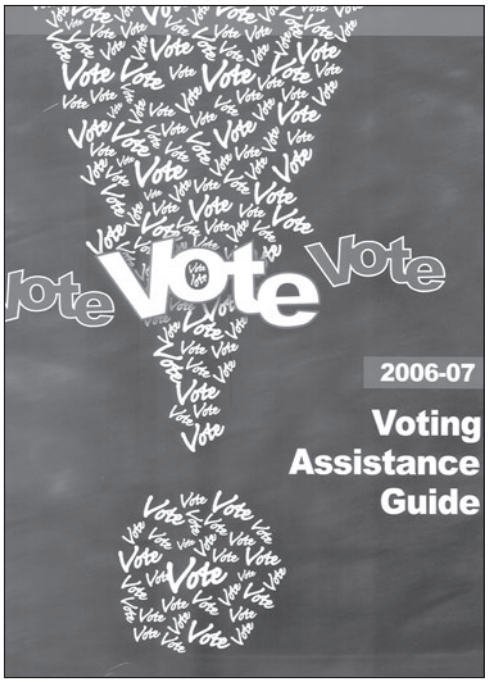
[31]DOD, *Report on IVAS 2006, As Required by Section 596 of the National Defense Authorization Act for Fiscal Year 2007*, December 2006.

[32]FVAP reported that states and territories allowing e-mail of the ballot request include Alaska, Colorado, Illinois, Indiana, Iowa (2006 only), Minnesota, Mississippi, Montana, North Carolina, North Dakota, Oregon, Puerto Rico, South Dakota, Virginia, Washington, and Wisconsin.

[33]As reported by FVAP, 7 states require the full Social Security number, 41 require the last 4 digits or driver's license, and 7 do not require the Social Security number.

[34]DOD established this Web site in 1995.

Figure 2: DOD's 2006-2007 Voting Assistance Guide



Source: DOD.

This guide tells the UOCAVA voter how to register, request a ballot, receive a ballot, and vote the ballot electronically—including by e-mail or fax—where state or territory law allows this. One link on FVAP's Web site had a full-text version of the guide, so that a Voting Action Officer[35] or other user could download and print the entire guide and use it to provide assistance to absentee voters from various states and jurisdictions. Another link goes to a Web page containing "State-by-State Instructions," where two additional links—one a PDF guide, the other an HTML version[36]—are provided for each state or territory. This allows voters to read or print off only their own state's or territory's instructions and to

[35]Service Voting Action Officers, for example, are responsible for voting assistance operations within their service.

[36]PDF means Portable Document Format; it is a file that is used to view electronic copies of paper documents, which allow an exact copy of the paper document. HTML means Hypertext Markup Language and is used to structure and format documents to be displayed on the World Wide Web.

have a choice of formats.[37] Another link goes to the Integrated Voting Alternative Site—this site provides information for the 55 states and territories regarding the electronic ballot request and receipt options available to UOCAVA voters. FVAP's Web site also has another link to News Releases, which contains updates on changes to the guidance, including changes to state laws that affect UOCAVA voters. Finally, a link goes to FVAP's Voting Assistance Guide Errata Sheets—this contains changes that have been made to the archived Voting Assistance Guide since its last printing.

Our review of the FVAP Web site, however, revealed inconsistencies in some of the information about electronic transmission options that the voters could access through different links on the site. Our analysis specifically showed that, while not widespread, for 14 of the 55 states or territories, some of the guidance regarding requirements for electronic transmission was inconsistent and could be misleading, as the following examples illustrate:

- For the state of California, we found that three of the FVAP links correctly stated that only overseas military and overseas civilian voters were eligible to receive or return a ballot by fax; a fourth link, however, did not include this restriction. As a result, military personnel stationed in the United States, but away from their state of residence, might conclude—incorrectly—that they were eligible to vote by fax. FVAP officials acknowledged this discrepancy and updated the information reached from the fourth link on January 25, 2007, to reflect the fact that uniformed servicemembers must be residing or deployed overseas to be able to receive and send ballots by fax.

- For the state of Colorado, we identified a news release that was issued on October 18, 2006, announcing a new initiative to allow uniformed servicemembers deployed outside the United States to request, receive, and return absentee ballots via e-mail. One other FVAP link reflected this change; however, four other links did not capture this change. FVAP officials acknowledged this discrepancy, updated two of the links, and

[37]The Executive Branch's "Access Board," which consists of cabinet-level officials from twelve federal agencies, among others, developed standards to implement section 508 of the Rehabilitation Act, which required federal agencies to have electronic information that is accessible to people with disabilities on government Web sites. FVAP stated that they provide access to an HTML version of their Voting Assistance Guide on their Web site to comply with this act. They also provide a PDF format of the Voting Assistance Guide for UOCAVA voters.

issued an errata sheet on January 22, 2007. FVAP officials did not update the third link—the 2006-2007 Voting Assistance Guide accessed through the publications link on their Web site—stating that it was considered an archive document and was not intended for update. However, DOD did not clearly identify this link as an archived document; as a result, this link could mislead voters who relied on it. FVAP officials later acknowledged that the archived version of the 2006-2007 Voting Assistance Guide could have been labeled better, and eventually deleted this version from their Web site.

Appendix II provides details on the inconsistencies we found on FVAP's Web sites for 14 states and identifies the links, along with DOD's responses regarding each. Under internal control guidance, organizations are to apply policies and procedures consistently.[38] As noted previously, while the inconsistencies were not widespread, the fact that inconsistencies exist at all could lead UOCAVA voters— especially busy voters residing or deployed in remote locations—to rely on incorrect information and therefore adversely affect their ability to vote. Agency officials acknowledged these discrepancies and addressed them during the course of our review.

Online Voting Forms

In addition, FVAP administers two online forms, (1) the Federal Post Card Application, which allows absentee voters to register to vote or request ballots; and (2) the Federal Write-in Absentee Ballot, which allows absentee voters to vote even if they have not yet received the absentee ballot they requested from their state or territory. The Federal Post Card Application has been online since 1999, in PDF format, and is postage-free within the U.S. mail system when appropriate markings, provided on FVAP's web site, are used. The online Federal Post Card Application allows voters to download a PDF version to their computers to complete, e-mail, print, sign, and send to their local election official via mail. Some state and local election officials we spoke with indicated that the online version of the Federal Post Card Application has many benefits because it is easy to fill out and read, and it provides sufficient space for the voter to write in.

[38]GAO, *Assessing Internal Controls in Performance Audits*, GAO/OP-4.1.4 (Washington, D.C.: September 1990) and *Standards for Internal Control in the Federal Government (Exposure Draft)*, GAO/AIMD-98-21.3.1 (Washington, D.C.: December 1997).

A UOCAVA voter can also use the Federal Write-in Absentee Ballot as a backup ballot when the state or territory has not sent a regular absentee ballot in time for the voter to participate in the election. On October 21, 2004, just a few weeks before the national election, FVAP issued a news release announcing the electronic version of the ballot as an emergency ballot. The Ronald W. Reagan NDAA for Fiscal Year 2005 amended the eligibility criteria in UOCAVA[39] to allow states and territories to accept the Federal Write-in Absentee Ballot under a broader range of circumstances. Prior to the change, a UOCAVA citizen had to be outside of the United States, have applied for a regular absentee ballot early enough to meet state election deadlines, and not have received it from the state. Under the new criteria, the Federal Write-in Absentee Ballot can be used by military servicemembers and their dependents stationed in the United States, as well as by military personnel, their dependents, and citizens living overseas.

Absence of Internet Absentee Voting Guidelines Has Hindered Development of the Mandated Internet-Based Absentee Voting Demonstration Project

The Election Assistance Commission has not yet developed the Internet absentee voting guidelines, and because it is required by law to develop them for DOD's use in the secure, Internet-based, absentee voting demonstration project, DOD has not moved ahead with the project. Commission officials told us that they have not yet developed the required Internet absentee voting guidelines because the Commission has been working on other priorities—including standards for electronic voting machines, challenges associated with these electronic voting machines, and a process for certification and accreditation—and it lacks the resources to work on the Internet absentee voting guidelines or the mandated study of the issues and challenges for Internet technology at the same time. Although the Internet voting study is now underway, the Commission has said that it will not be completed until September 2007 and thus does not have the results it needs to establish time frames or a plan for developing the guidelines. Regarding the demonstration project, DOD officials stated that they had not taken action to develop this project because the Ronald W. Reagan NDAA for Fiscal Year 2005 requires the Commission to develop the guidelines first. DOD officials stated that, in an effort to assist the Commission in developing the Internet absentee voting guidelines, they have provided information on prior Internet voting efforts, along with challenges associated with these Internet voting efforts and views on how to mitigate those challenges.

[39]Pub. L. No. 108-375 § 566(c) (2004).

The Commission Has Not Developed Internet Absentee Voting Guidelines because of Other Priorities, Constraints on Resources, and Lack of DOD Information

Commission officials stated that they have not developed Internet absentee voting guidelines because the Commission and the organizations that would normally provide assistance to it are directing their constrained resources to other priorities. This includes addressing challenges associated with electronic voting machines and establishing a process for certification and accreditation. Additionally, the Help America Vote Act of 2002 requires the Commission's Technical Guidelines Development Committee to assist the Executive Director of the Commission in developing voluntary voting system guidelines.[40] The act also requires the Director of the National Institute of Standards and Technology to provide the Development Committee with technical support in developing those guidelines, including research and development related to computer and network security, voter privacy, remote access voting (including voting through the Internet), and voting fraud.

Commission officials told us, however, that the Development Committee has not been able to work on Internet absentee voting guidelines for UOCAVA voters because it had other priorities and constraints on its resources.[41] In light of the Development Committee's low priority for working on the Internet absentee voting guidelines, officials from the Commission asked officials from the National Institute of Standards and Technology to assist with developing the guidelines. However, officials from the National Institute of Standards and Technology said that they could not provide support because they also lacked sufficient resources at the time. Commission officials told us that, at the time of our review, the National Institute of Standards and Technology was also using its resources to work with the Development Committee on the current voluntary voting guidelines and would not have sufficient resources to work on Internet absentee voting guidelines until after July 2007.

Additionally, Commission officials stated that they were waiting for DOD to provide information that describes the type of system around which the

[40]These guidelines provide a set of specifications and requirements to be used in the certification of computer-assisted voting systems, both paper-based and fully electronic, and are voluntary—that is, states are free to adopt them in whole or in part or to reject them entirely.

[41]For example, Commission officials told us that the Development Committee is working on updates to the Voluntary Voting System Guidelines that were established in 2005. These guidelines will become effective December 2007. The guidelines focus primarily on electronic voting machines and ballot counters, but not on Internet voting systems for UOCAVA voters.

guidelines should be developed. DOD officials, however, stated that they gave the Commission reports that provided the framework for the Internet-based absentee voting system they envisioned. Specifically, these DOD officials told us that they provided the Commission, in 2004, with a report on their 2000 proof of concept for Internet-based voting called "Voting Over the Internet,"[42] and in March 2006, they provided the Commission with an internal DOD document assessing the terminated SERVE project. DOD and Commission officials told us that they had not communicated in depth on the guidelines and the DOD system before our review.

The Election Assistance Commission Has Started a Study as a Precursor to the Internet Absentee Voting Guidelines

To gain a better understanding of the Internet voting environment, in September 2006, the Commission started an Internet voting study as a precursor to developing the Internet absentee voting guidelines. The Help America Vote Act of 2002 required the Commission to conduct this study to determine the issues and challenges presented by incorporating communications and Internet technology into elections, including the potential for election fraud, and to issue a report no later than June 29, 2004. However, the Commission did not meet this reporting date. Commission officials told us that they were unable to complete the study sooner—or even begin it—because of the resource constraints they have worked under since the Commission's inception, and because they were working on other priorities. They noted, for example, that under the act, the Commission was to be established by February 26, 2003, but the Commissioners were not appointed until almost a year later, in December, 2003. They also told us that, although 23 employees were allocated to the Commission, they had to build up staff gradually, starting in January 2004, by hiring two employees each month. Accordingly, Commission officials testified in June 2004[43] that, as a result of these constraints, the Commission was able to meet only some of its mandates, such as developing the 2005 Voluntary Voting System Guidelines. As a result, the Commission was not able to conduct the Internet voting study in a timely manner.

[42]Department of Defense, *Federal Voting Assistance Program: Voting Over the Internet*, June 2001.

[43]*Statement of U.S. Election Assistance Commission before the U.S. House Of Representatives, Committee on House Administration*, dated June 17, 2004.

Commission officials stated that the Internet voting study, which was underway during the course of our review, includes several case studies to monitor current Internet voting usage and electronic transmission of ballots. The four states participating in this part of the study are Florida, Montana, South Carolina, and Illinois. The study also includes (1) a survey of UOCAVA voters to collect information on their level of interest in electronic voting and (2) a conference to gather states' experiences on topics such as Internet voting, electronic transmission of ballots, security risks for voting systems, and verification of voters' identities. Commission officials told us that they plan to issue a final report on the Internet voting study in September 2007.

The Commission Does Not Have a Plan for Assessing Security Issues and Developing Internet Absentee Voting Guidelines

The Ronald W. Reagan NDAA for Fiscal Year 2005 did not establish a deadline by which the Commission was to complete the Internet absentee voting guidelines, and the Commission has not set time frames for itself, primarily because it has been working on guidelines for current voting systems. Additionally, as stated previously, the Commission has not completed the precursor Internet voting study to identify critical issues and challenges such as those related to security and privacy. Also, it has not established a plan, in conjunction with major stakeholders like DOD, to develop appropriate guidelines for Internet voting with specific tasks that would address security risks such as those identified in its study and other security evaluations and reports, as well as time frames and milestones.

In previous reports, we have noted that leading organizations develop long-term results-oriented plans that involve all stakeholders and identify specific tasks, milestones, time frames, and contingency plans;[44] this practice is also embodied in the underlying principles of the Government Performance and Results Act of 1993.[45] Similarly, without a plan for the UOCAVA Internet absentee voting guidelines—including specific tasks, time frames, milestones, necessary resources, and alternatives—the Commission cannot inform Congress, FVAP, and local election officials when it will meet the mandate to develop the required guidelines. As we

[44]GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, GAO-GGD-96-118 (Washington, D.C.: June 1996) and *Military Readiness: Navy's Fleet Response Plan Would Benefit from a Comprehensive Management Approach and Rigorous Testing*, GAO-06-84 (Washington, D.C.: Nov. 22, 2005).

[45]Pub. L. No. 103-62 (1993).

previously noted, some technologies may not yet be mature enough to support Internet voting. Therefore, the plan for developing Internet absentee voting guidelines may require an incremental approach that reflects emerging solutions to security and privacy challenges, as well as changing views on acceptable levels of risk and cost.

DOD Has Not Developed a Secure, Internet-based, Absentee Voting Demonstration Project

Similarly, DOD has not developed a secure, Internet-based absentee voting demonstration project, as Congress mandated in the Ronald W. Reagan NDAA for Fiscal Year 2005. DOD reported that the principal objective of the Internet-based electronic demonstration project was to assess the use of such technologies to improve UOCAVA participation in elections. The department planned to conduct the project during the first general election for federal office after the Commission has established Internet voting guidelines for the project. However, DOD has not moved forward with the electronic demonstration project because, by law, the Commission must first develop the Internet absentee voting guidelines.

DOD officials stated, as mentioned previously, that they provided information to assist the Commission in developing the guidelines, and Commission officials acknowledged that DOD had provided them with a report on "Voting Over the Internet," DOD's assessment of its November 2000 Internet-based voting project, in 2004—the first year of the Commission's operation. DOD also provided the Commission with an internal document that contained information on its SERVE project. However, Commission officials told us that they did not receive the SERVE document until June 2006. This document discussed challenges DOD identified with Internet voting, which included security threats such as computer viruses, malicious insider attacks, and inadvertent errors that could disrupt system performance.

In 2001, we also identified several challenges to Internet voting, such as privacy and security.[46] As previously mentioned, we reported that broad application of Internet voting faced formidable challenges, including the difficulty of providing adequate voter privacy—that is, protecting the voter's ability to cast a ballot without being observed. We further reported that, although not unanimous on all issues, groups considering the pros and cons of Internet voting were in consensus in identifying security as the primary technical challenge for Internet voting. We also reported that,

[46] GAO-01-1026; GAO-02-3.

because of the security risks involved, Internet voting would not likely be implemented on a large scale in the near future. Moreover, DOD officials told us that even if the Commission had developed Internet voting guidelines at the time of our review, DOD would not have been able to develop a secure, Internet-based, electronic demonstration project in time for the 2008 presidential election. DOD officials said that—depending on the Internet voting guidelines provided by the Commission—the final system design, full development, testing and deployment phases would take an estimated 24 to 60 months. Furthermore, deployment of any system requires participation of the military services, which have many additional, competing priorities that may cause delays in deployment. Given that less than 17 months remain before the November 2008 election, FVAP officials said there is insufficient time to advertise and launch the Internet-based electronic demonstration project.

DOD Was Developing Plans to Expand the Use of Electronic Voting Technology in the Future, but Sound Management Practices Are Key

We observed that DOD was developing, but had not yet completed, plans to expand the use of electronic voting technology for UOCAVA voters use in federal elections through November 2010, as required by the John Warner NDAA for Fiscal Year 2007. DOD officials told us that they anticipated providing the plans to Congress, in accordance with the act, by May 15, 2007. Because electronic voting initiatives for the absentee voting process (fax, e-mail, and Internet) involve numerous stakeholders at the federal level—including DOD and the Commission—as well as the various state and local levels, developing a plan is key. Implementation of new electronic voting initiatives requires careful planning, particularly in light of the remote location of troops, the application of new technology, and the lead time required for implementation. As DOD develops these plans, employing a comprehensive strategic approach that incorporates sound management principles could provide a framework for DOD's plans. Our analyses of DOD and Commission documents and our interviews—including those with officials from these agencies, organizations representing UOCAVA voters, and state and local election officials—show that DOD did not obtain sufficient stakeholder involvement in planning its recent electronic voting initiatives—the 2004 and 2006 IVAS initiatives. In fact, Commission officials mentioned that DOD's recent initiatives took a "top down" approach and did not seek input from the Commission or from local jurisdictions during the planning stage. DOD officials noted that both the 2004 and 2006 IVAS initiatives were planned, designed, advertised, and implemented just months before those two elections. In the case of the 2006 IVAS, however, the department reported that it developed the system within 79 days of passage of the mandate—June 2006—and noted that it was in fact responsive to that mandate. The Commission and state and

local election officials noted that the aggressive schedules for these latest electronic initiatives did not allow sufficient time to enable full participation, training, and dissemination of information on the efforts. Additionally, at the time of our review, DOD officials said they had not yet established interim tasks that address issues such as security and privacy, milestones, time frames, and contingency plans.

The principles of sound management used by leading organizations and embodied in the Government Performance and Results Act of 1993[47] provide a methodology to establish a results-oriented framework for DOD to develop its detailed plans. Such a framework would provide a firm foundation for DOD's long-term plan for electronic voting initiatives. Some of the key management principles include (1) involving stakeholders when defining the mission and outcomes, (2) identifying specific actions and tasks, such as monitoring and assessing security of the initiatives, (3) developing schedules and time frames for tasks, and (4) evaluating the overall effort, with specific processes to allow for adjustments and changes. Furthermore, as we reported in one of our executive guides, leading organizations plan for a continuous cycle of risk management. This includes determining needs, assessing security risks, implementing policies and controls, promoting awareness, and monitoring and evaluating controls.[48] Combined with effective leadership, these principles provide decision makers with a framework to guide program efforts and the means to determine if these efforts are achieving the desired results.

In its December 2006 report to Congress on IVAS,[49] DOD stated the following:

- Development of a long-term strategic plan was necessary to ensure that all related initiatives were effectively integrated, but this was dependent on having sufficient time to assess, improve, and evaluate new or evolving electronic alternatives.
- Major recommendations for its future electronic voting projects would include, for example,
  - recognizing the variation in state and local laws, procedures, and systems;

[47]Pub. L. No. 103-62 (1993). GAO/GGD-96-118.

[48]GAO, *Executive Guide: Information Security Management, Learning From Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

[49]DOD, *Report on IVAS 2006*.

- identifying and mitigating actual and perceived risks, by educating people about risk management practices; and
- building consensus among key stakeholders.

As stated previously, Commission officials told us that, for recent initiatives, DOD did not seek input from the Commission or local jurisdictions during the planning stage of these efforts. Without a proactive, integrated, long-term, results-oriented plan that involves all major stakeholders; includes goals, interim tasks—such as identifying security risks and addressing privacy concerns—milestones, time frames, and contingency plans; and follows the sound management practices used by leading organizations, DOD is not in a position to address congressional expectations to establish secure and private electronic and Internet-based voting initiatives.

Conclusions

It is imperative that the 6 million Americans who are covered under the Uniformed and Overseas Citizens Absentee Voting Act have the opportunity to exercise their right to vote—one of the hallmarks of a democratic society. The fact that time is an issue with absentee voting by regular mail has led many to look toward electronic and Internet voting, which represent the next generation of voting technology, as alternatives. While these alternatives may expedite the absentee voting process, they are more vulnerable to privacy and security compromises than the conventional methods now in use. Electronic and Internet voting require safeguards to limit such vulnerabilities and prevent compromises to votes from intentional actions or inadvertent errors. However, available safeguards may not adequately reduce the risks of compromise. To date, the Election Assistance Commission has not assessed the risks or possible safeguards for Internet voting, nor has it developed corresponding guidelines that define minimum Internet voting capabilities and safeguards to be considered by the election community. Furthermore, electronic and Internet-based absentee voting can be challenging for UOCAVA voters, who reside at multiple locations across the globe. These voters are also registered to vote in thousands of local jurisdictions across 55 states and territories that employ varying levels of technology—from paper ballots to faxes and e-mail. DOD faces significant challenges in leveraging electronic and Internet technology to facilitate this complex, global absentee voting process. Delays in developing guidelines and a demonstration project have resulted in two presidential elections passing without significant progress in moving toward expanded use of electronic and Internet absentee voting. DOD officials told us it is now too late in the cycle to implement significant changes before the 2008 election. The challenges of

coordinating among numerous stakeholders—including DOD, the Commission, and state and local election officials, as well as organizations representing UOCAVA voters—are substantial, and, to date, efforts to involve stakeholders in the planning stage of DOD's recent initiatives have fallen short. This delay has left an expectation gap between what Congress required and what has been accomplished so far. Several steps would have to be taken to overcome these challenges, including better coordination between the Commission and DOD regarding their complementary roles in developing Internet voting guidelines and the mandated demonstration project. Unless the Commission and DOD move in a timely manner to assess the technology risks, develop guidelines that address the risks, coordinate among election stakeholders, and establish and execute prudent plans, they are unlikely to meet the expectations of Congress and military and overseas voters to establish a secure and private electronic and Internet-based UOCAVA voting environment.

Recommendations for DOD

To improve the security and accuracy of DOD's electronic and Internet initiatives, we recommend that the Secretary of Defense direct the Under Secretary of Defense for Personnel and Readiness to take the following four actions:

- Comply with the information security requirements in the DOD Certification and Accreditation Process guidance.
- Incorporate lessons learned into plans for future systems such as those we identified, including adding cautionary statements to future ballot request and receipt systems to warn UOCAVA voters to remove personal data from their computers.
- Institutionalize a process to review online UOCAVA guidance to ensure that DOD provides accurate and consistent information to UOCAVA voters.
- Create an integrated, comprehensive, long-term, results-oriented plan for future electronic voting programs that specifies, among other things, the goals to be achieved along with tasks including identifying safeguards for the security and privacy of all DOD's voting systems—both electronic and Internet. The plan should also specify milestones, time frames, and contingencies; synchronize them with planned development of the Commission's guidelines for Internet voting; and be developed in conjunction with major stakeholders—including state and local election officials, the Election Assistance Commission, overseas voting groups, and each of the armed services. The plan should also include initiatives that will be done well in advance of federal elections, to allow adequate time

for training and dissemination of information on the options available to UOCAVA voters.

Recommendations for the Election Assistance Commission

To improve the Election Assistance Commission's efforts to comply with the direction from Congress to develop the Internet absentee voting guidelines, we recommend that the Commission take the following two actions:

- Determine, in conjunction with major stakeholders like DOD, whether the Commission's 2007 Internet voting study and any other Commission efforts related to Internet or electronic voting are applicable to DOD's plans for Internet-based voting, and incorporate them where appropriate.
- Develop and execute, in conjunction with major stakeholders—including state and local election officials and DOD—a results-oriented action plan that specifies, among other things, goals, tasks, milestones, time frames, and contingencies that appropriately address the risks found in the UOCAVA voting environment—especially risks related to security and privacy.

Agency Comments and Our Evaluation

In written comments on a draft of this report, DOD concurred with our recommendations to (1) comply with the information security requirements, (2) incorporate lessons learned into plans for future systems—to include adding cautionary statements to warn UOCAVA voters to remove personal data from their computers, (3) institutionalize a process to review online UOCAVA guidance, and (4) create a comprehensive, results-oriented, long-term plan for future electronic voting initiatives. The department said that it will contract for services to comply with the information security requirements and will incorporate identified lessons learned into future registration, ballot request, and ballot receipt systems. The department said that it has already streamlined its online guidance by, among other things, eliminating the archived "Publications" version of the Voting Assistance Guide entirely; it will also establish a revised review process for online information. DOD noted that these changes will reduce the possibility of human error and simplify the review and verification process of online information. Finally, DOD stated that it was in full support of a long-term, comprehensive plan for future electronic voting projects that would allow for sufficient time to involve the major stakeholders, train, and disseminate information and ultimately serve UOCAVA voters. The department said it looked forward to working on this multiyear project plan in cooperation with the Election Assistance Commission, the National Institute of Standards and Technology, and

other major stakeholders. It further stated that FVAP, the Commission, and the National Institute of Standards and Technology are scheduling a meeting to lay the groundwork for the plan. DOD's comments are reprinted in appendix III. DOD also provided technical comments, which we incorporated in the final report, as appropriate.

In its written comments, the Election Assistance Commission concurred with our recommendations to (1) determine the applicability of the Commission's 2007 Internet voting study and other Commission studies to DOD's plans for Internet-based voting, and (2) develop and execute a results-oriented action plan to provide guidelines that appropriately address the risks found in the UOCAVA voting environment. The Commission stated that it has already met with FVAP and the National Institute of Standards and Technology and agreed to develop a time line for creating the UOCAVA guidelines. The Commission's comments are reprinted in appendix IV.

We are sending copies of this report to the Secretary of Defense and the Under Secretary of Defense (Personnel and Readiness) and the Commissioners of the Election Assistance Commission. We will also make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

Should you or your staff have any questions about this report, please contact me at (202) 512-5559. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix V.

Derek Stewart
Director, Defense Capabilities and Management

Appendix I: Scope and Methodology

To assess DOD's electronic initiatives, we reviewed and analyzed relevant laws, directives, and guidance. These included DOD Directive 1000.4, Federal Voting Assistance Program (FVAP), updated April 14, 2004; and *DOD's Interim Department of Defense (DOD) Certification and Accreditation (C&A) Process Guidance*, dated July 6, 2006. We also reviewed applicable requirements documents for DOD's electronic efforts, as well as relevant reports by GAO, DOD, FVAP, the DOD Inspector General, and others, including *A Security Analysis of the Secure Electronic Registration and Voting Experiment* (SERVE), dated January 21, 2004. In addition, we reviewed FVAP's 2006-2007 Voting Assistance Guide and its Web site to ascertain what type of information on electronic voting alternatives is provided to UOCAVA citizens.

We interviewed key program officials at the Office of the Under Secretary of Defense for Personnel and Readiness's Federal Voting Assistance Program (FVAP), the Business Transformation Agency, the Defense Manpower Data Center, and Voting Action Officers from several service headquarters. We also contacted officials from (1) election organizations, including the National Association of Secretaries of State and Joint Election Officials Liaison Committee and (2) organizations representing UOCAVA voters, including those from the National Defense Committee and the Overseas Vote Foundation. We made contact with officials from 14 of the 16 state and local election offices we called to obtain their perspectives on DOD's initiatives. Specifically, we included all 11 states that had participated in DOD's 2006 Integrated Voting Alternative Site—some of which participated in SERVE and other DOD programs and initiatives. We also included three other states that had 10 or more military bases and had participated in SERVE though not in IVAS. Table 3 lists the states we contacted and the programs in which these states participated.

Table 3: State Offices Contacted and Programs Where the States Were Participants

	States contacted	SERVE participants[a]	IVAS Tool 1 participants[a]	IVAS Tool 2 participants[a]
1	Arkansas	Yes	Yes	No
2	Florida	Yes	No	No
3	Hawaii	Yes	No	No
4	Illinois	No	Yes	No
5	Indiana	No	No	Yes
6	Kentucky	No	No	Yes
7	Mississippi	No	Yes	No
8	Montana	No	No	Yes
9	North Carolina	Yes	Yes	No
10	Puerto Rico	No	Yes	No
11	South Carolina	Yes	No	No
12	Vermont	No	Yes	No
13	Virgin Islands	No	Yes	No
14	Washington	Yes	Yes	No
Totals	**14 states contacted**	**6 SERVE states contacted**	**8 IVAS Tool 1 states contacted**	**3 IVAS Tool 2 states contacted**

Source: GAO analysis of DOD data.

[a]While a number of jurisdictions were included under each of the DOD programs listed, we spoke to at least one election official from each state.

To determine the Commission's efforts to develop Internet voting guidelines and DOD's efforts to develop the secure, Internet-based, absentee voting demonstration project, we reviewed and analyzed relevant laws, Commission reports, and to the extent they existed, the Commission's strategic plan and other documents to ascertain its plans and efforts to develop Internet voting guidelines for UOCAVA voters. We also reviewed and analyzed various DOD requirements documents, GAO reports, internal DOD reports, and other reports related to DOD's prior Internet-based absentee voting initiatives—Voting Over the Internet and SERVE—to ascertain, among other things, challenges and benefits associated with Internet voting efforts. Additionally, we interviewed key program officials within FVAP, including the Director and Deputy Director of FVAP and the Project Manager for SERVE, who is currently retired, along with officials on DOD's private sector Security Peer Review Group. We also spoke with officials on the Commission's Technical Guidelines

Development Committee and with the National Institute of Standards and Technology.

To ascertain DOD's efforts to develop plans to expand the use of electronic voting technologies in the future, we reviewed and analyzed laws, guidance, and reports to determine DOD's current and future plans for the Internet-based absentee voting demonstration project. Additionally, we examined, to the extent they existed, DOD's strategic plan and other documentation to determine its current and future plans for the Internet-based absentee voting demonstration project. We also interviewed responsible officials within DOD about these plans—including the Principal Deputy Under Secretary of Defense for Personnel and Readiness and the Director and Deputy Director of FVAP.

We conducted our work from August 2006 through April 2007 in accordance with generally accepted government auditing standards.

Appendix II: Examples of the Inconsistent Voting Assistance Guidance on DOD's Web Site

During the course of our review, we compared and analyzed the voting assistance guidance provided on DOD's Federal Voting Assistance Program (FVAP) Web site that covered electronic alternatives to mail. The online links we reviewed included FVAP's: (1) 2006-2007 Voting Assistance Guide (VAG)—a PDF version;[1] (2) 2006-2007 VAG—an HTML version;[2] (3) the archived 2006-2007 VAG—a PDF version dated October 25, 2005;[3] (4) changes to the archived 2006-2007 VAG—called Errata Sheets; (5) News Releases; and (6) the 2006 Integrated Voting Alternative Site (IVAS). While not widespread, for 14 of the 55 states and territories, we found differences in some of the guidance provided on these links.[4] Table 4 shows the differences we identified.

Table 4: Inconsistencies Identified in Guidance on Electronic Alternatives to Mail

	State	Differences identified	Questions	FVAP response	GAO observation
1	California	Both PDF versions and the HTML Voting Assistance Guides state that only overseas military and overseas citizens may receive and send the ballot by fax. IVAS instruction does not restrict who can receive or send the ballot by fax.	Could an absentee ballot sent by fax by military personnel within the United States be rejected if a voter covered under the Uniformed and Overseas Citizens Absentee Voting Act relied solely on IVAS for voting guidance?	IVAS page was incorrect and was updated on1/25/07. The instruction should have specified that Uniformed Servicemembers must be overseas to receive and send the ballot by fax. By law, an absentee ballot faxed from within the United States should be rejected.	Correction to IVAS has been verified.

[1]PDF means Portable Document Format; it is a file format that is used to view electronic copies of paper documents, which allows an exact copy of the paper document.

[2]HTML means Hypertext Markup Language and is used to structure and format documents to be displayed on the World Wide Web.

[3]This 2006-2007 VAG was accessed at http://www.fvap.gov/pubs/vag/pdfvag/2006-07vag.pdf; but DOD deleted this link in February 2007.

[4]We found 16 instances in total. Two of the states had two separate discrepancies identified.

	State	Differences identified	Questions	FVAP response	GAO observation
2	Colorado	The News Release for Colorado on October 18, 2006, and IVAS "allow Uniformed Servicemembers deployed outside the U.S. to request, receive, and return absentee ballots via e-mail." This is not reflected in the two PDF versions or HTML Voting Assistance Guides, nor was an errata sheet created.	Would overseas uniformed voters know of the e-mail options if they relied on the Voting Assistance Guide for voting guidance?	The Voting Assistance Guide, PDF, HTML, and errata sheet have been updated to reflect the change. Web site changes to the Voting Assistance Guide were made January 22, 2007.	Corrections to PDF, HTML, and errata sheet have been verified. FVAP stated that the "Publications" version of the Voting Assistance Guide in PDF format was the original book version of the Guide in electronic form. Since it was considered an archived document, FVAP officials stated that it was not intended for update; but, acknowledged that this version could have been marked better as an archived document. These officials have since deleted this version of the Guide from their Web site.
3	Illinois	FVAP issued an errata sheet for Illinois on September 29, 2006, and all changes except one are reflected in the HTML and PDF "Publications" versions of the Voting Assistance Guide and IVAS did not mention the change. Specifically, the change that is not captured is in Item IIE (Uniformed Services): "The Publications" PDF and HTML Voting Assistance Guides say Illinois does not allow receipt of blank ballots by fax or e-mail and IVAS does not address this issue.	Would uniformed voters be aware of the fax and e-mail provisions if they relied on IVAS, HTML Voting Assistance Guide, or "publications" PDF version?	The fax and e-mail provisions on the errata sheet and the Voting Assistance Guide PDF are correct as accepted by the State of Illinois. The IVAS page and the Voting Assistance Guide HTML were missing the information about the City of Chicago and Suburban Cook County allowing receipt of the blank ballot by fax or e-mail. The information was added on both the IVAS and the HTML on January 26, 2007. See note below on "Publications" version of the Voting Assistance Guide.[a]	Corrections to IVAS and HTML have been verified. FVAP officials acknowledged that the "Publications" version of the Voting Assistance Guide could have been marked better as an archived document, and have since deleted this version of the Guide from their Web site.

	State	Differences identified	Questions	FVAP response	GAO observation
4	North Carolina	FVAP issued a News Release and updated IVAS on October 20, 2006, stating that North Carolina now allows all citizens covered under the Uniformed and Overseas Citizens Absentee Voting Act to, among other things, receive blank absentee ballots and return voted ballots by fax. It also stated that the Federal Post Card Application could be faxed or e-mailed. This information was not reflected in the FVAP PDFs or HTML versions of the Voting Assistance Guide, nor was an errata sheet created.	Would voters covered under the Uniformed and Overseas Citizens Absentee Voting Act know of the fax or e-mail options if they relied on the Voting Assistance Guide publications?	Voting Assistance Guide pages updated to reflect information contained in News Release on January 29, 2007. See note below on "Publications" version of the Voting Assistance Guide.[a]	Corrections to PDF and HTML Voting Assistance Guide and errata sheet have been verified. FVAP officials acknowledged that "Publications" version of the Voting Assistance Guide could have been marked better as an archived document, and have since deleted this version of the Guide from their Web site.
5	Rhode Island	Rhode Island's Overseas Civilians instructions for FVAP's PDFs and HTML Voting Assistance Guide include language in Section IIIB stating that ballots "may be requested by using the Federal Post Card Application, letter, telephone, fax, or e-mail." This language contradicts guidance in Section IIIE of the HTML and PDF Voting Assistance Guides which only mentions fax transmissions. Furthermore, the IVAS Web site says no e-mail is permitted.	Would overseas civilians know of the option to request the blank ballot by e-mail if they relied on Section IIIE of the Voting Assistance Guide or IVAS?	The language in question does not refer to the ability of the voter to request an absentee ballot via e-mail, but to request that a copy of a state form (now discarded) be sent to them, which could be requested by using a Federal Post Card Application, via fax, e-mail, phone, etc. Given that the state form has been discarded, the Voting Assistance Guide has been updated to reflect the change. Web site changes to the Voting Assistance Guide were made January 29, 2007.	Corrections to the PDF, HTML, IVAS, and errata sheet have been verified.

	State	Differences identified	Questions	FVAP response	GAO observation
6	South Dakota	South Dakota's errata sheet from June 19, 2006 and the PDF Voting Assistance Guide require the Federal Post Card Application be notarized for stateside military voters. This is not mentioned as a requirement in IVAS, or the HTML or "Publications" Voting Assistance Guide. (Specifically, these say that "no registration or voting materials are notarized or witnessed.")	Would stateside military voters know that they are required to have the Federal Post Card Application notarized if they rely on IVAS, HTML or "Publications" Voting Assistance Guides instead of the errata sheet?	The change was made by South Dakota and approval signed. The PDF and errata sheet were changed, the HTML was overlooked, and correction was made January 26, 2007. The IVAS page did not contain full instructions but referred the reader to the Voting Assistance Guide instructions. See note below on "Publications" version of the Voting Assistance Guide.[a]	Correction to the HTML has been verified. IVAS referred the voter to the Voting Assistance Guide instructions. FVAP officials acknowledged that "Publications" version of the Voting Assistance Guide could have been marked better as an archived document, and have since deleted this version of the Guide from their Web site.
7	South Dakota	South Dakota's errata sheet from October 4, 2006, and HTML and PDF Voting Assistance Guides allow voters covered under the Uniformed and Overseas Citizens Absentee Voting Act to send the Federal Post Card Application by fax and allow a voter to submit a scanned application as an e-mail attachment. This is not reflected in the "Publications" Voting Assistance Guide.	Would voters covered under the Uniformed and Overseas Citizens Absentee Voting Act know of the option to send the Federal Post Card Application by fax or via e-mail attachment if they relied on the "Publications" Voting Assistance Guide?	See note below on "Publications" version of the Voting Assistance Guide.[a]	FVAP officials acknowledged that "Publications" version of the Voting Assistance Guide could have been marked better as an archived document, and have since deleted this version of the Guide from their Web site.
8	Utah	Utah's errata sheet from May 11, 2006, and PDF Voting Assistance Guide (uniformed services) states that registration and voting materials are not notarized or witnessed. This is not reflected in the HTML or PDF "Publications" version of the Voting Assistance Guide. For example, the HTML Voting Assistance Guide says that no notary or witness is required, but mentions certification.	Would uniformed voters know that they were not required to have their voting materials notarized if they relied on the HTML or "Publications" Voting Assistance Guide?	Change was made to reflect Utah's election law and approval signed. The PDF and errata sheet were corrected, however, the HTML was overlooked. Correction was made January 26, 2007. See note below on "Publications" version of the Voting Assistance Guide.[a]	Correction to the HTML has been verified. FVAP officials acknowledged that "Publications" version of the Voting Assistance Guide could have been marked better as an archived document, and have since deleted this version of the Guide from their Web site.

	State	Differences identified	Questions	FVAP response	GAO observation
9	Vermont	While the notary section of Civilian Outside U.S. in the PDF Voting Assistance Guide has the statement about witness requirements for the return ballot, it does not have the statement: "However, your signature must be on the inside envelope certificate." This line is reflected in the HTML Voting Assistance Guide and in all notary sections of the Uniformed Services Voting Assistance Guides.	Would overseas civilians know that their signature is required on the inside envelope certificate if they relied on the PDF Voting Assistance Guide?	The PDF Voting Assistance Guide had the signed approval of Vermont. The missing line was simply overlooked by the state and FVAP and was updated on January 25, 2007.	Correction to the PDF has been verified.
10	Alaska	The HTML, "State-by-State" PDF Voting Assistance Guide, and IVAS instruction allow e-mailing of the blank ballot and voted ballot. This is not reflected in the "Publications" version of the PDF Voting Assistance Guide for Alaska.	Would voters covered under the Uniformed and Overseas Citizens Absentee Voting Act know of the option to e-mail the blank and voted ballot if they relied on the "Publications" Voting Assistance Guide?	See note below on "Publications" version of the Voting Assistance Guide.[a]	FVAP officials acknowledged that "Publications" version of the Voting Assistance Guide could have been marked better as an archived document, and have since deleted this version of the Guide from their Web site.
11	Oregon	An errata sheet on August 22, 2006 for Oregon and the HTML and PDF Voting Assistance Guides added, in addition to faxing, the words "or e-mail" to the electronic transmission sections in the Voting Assistance Guide. This information is not reflected in the "Publications" version of the Voting Assistance Guide.	Would voters covered under the Uniformed and Overseas Citizens Absentee Voting Act know of the option to use e-mail for their voting materials if they relied on the "Publications" Voting Assistance Guide?	See note below on "Publications" version of the Voting Assistance Guide.[a]	FVAP officials acknowledged that "Publications" version of the Voting Assistance Guide could have been marked better as an archived document, and have since deleted this version of the Guide from their Web site.
12	South Carolina	An errata sheet and a news release on May 5, 2006 and the HTML and PDF Voting Assistance Guides announced that voters are allowed to receive and return the ballot by fax or e-mail under any conditions or circumstances. This information is not reflected in the "Publications" version of the Voting Assistance Guide, which only allows fax and e-mail for emergencies.	Would voters covered under the Uniformed and Overseas Citizens Absentee Voting Act know of the fax and e-mail options if they relied on the "Publications" Voting Assistance Guide?	See note below on "Publications" version of the Voting Assistance Guide.[a]	FVAP officials acknowledged that "Publications" version of the Voting Assistance Guide could have been marked better as an archived document, and have since deleted this version of the Guide from their Web site.

	State	Differences identified	Questions	FVAP response	GAO observation
13	Texas	FVAP issued an errata sheet for Texas on July 24, 2006, that changed the first bullet in both electronic transmission sections, which says Texas allows voters to send the Federal Post Card Application by fax; but adds "to request an absentee ballot and for temporary registration only." This information was in the HTML and PDF Voting Assistance Guides but is not reflected in the "Publications" version of the Voting Assistance Guide.	Would voters covered under the Uniformed and Overseas Citizens Absentee Voting Act know the fax option was for only to request the ballot and temporary registration, if they relied on the "Publications" Voting Assistance Guide?	See note below on "Publications" version of the Voting Assistance Guide.[a] The state of Texas only allows faxing to be used to request a ballot and for temporary registration. It is not allowed for the use of permanent registration. The impact on voters may be negligible as these voters still receive ballots for two successive election cycles.	FVAP officials acknowledged that "Publications" version of the Voting Assistance Guide could have been marked better as an archived document, and have since deleted this version of the Guide from their Web site.
14	Virginia	An errata sheet for Virginia on July 20, 2006, and the HTML and PDF Voting Assistance Guides allow only overseas military members to receive the blank ballot by e-mail or fax upon request. This information is not reflected in the "Publications" version of the Voting Assistance Guide.	Would stateside military members know of the stipulation that only overseas military members may receive the blank ballot by e-mail or fax if they relied on the "Publications" Voting Assistance Guide?	See note below on "Publications" version of the Voting Assistance Guide.[a]	FVAP officials acknowledged that "Publications" version of the Voting Assistance Guide could have been marked better as an archived document, and have since deleted this version of the Guide from their Web site.
15	Virginia	An errata sheet for Virginia on July 20, 2006, and the HTML and PDF Voting Assistance Guides changed the Civilian language to "Some Virginia counties and cities allow you to receive the blank ballot by e-mail or fax upon request." This limiting information "some" is not reflected in the "Publications" version of the Voting Assistance Guide. It simply says that Virginia "allows you to receive the blank ballot you e-mail or fax upon request."	Would overseas civilians know of the stipulation that only some Virginia counties and cities allow receipt of the blank ballot by fax or e-mail if they relied on the "Publications" Voting Assistance Guide?	See note below on "Publications" version of the Voting Assistance Guide.[a]	FVAP officials acknowledged that "Publications" version of the Voting Assistance Guide could have been marked better as an archived document, and have since deleted this version of the Guide from their Web site.

	State	Differences identified	Questions	FVAP response	GAO observation
16	Wisconsin	FVAP issued an errata sheet on July 24, 2006 for Wisconsin allowing voters to send the Federal Post Card Application for absentee ballot request by fax or e-mail. This information is not reflected in the "Publications" Voting Assistance Guide.	Would voters covered under the Uniformed and Overseas Citizens Absentee Voting Act know of the option to send the Federal Post Card Application by fax or e-mail if they relied on the "Publications" Voting Assistance Guide instead of the errata sheet?	See note below on "Publications" version of the Voting Assistance Guide.[a]	FVAP officials acknowledged that "Publications" version of the Voting Assistance Guide could have been marked better as an archived document, and have since deleted this version of the Guide from their Web site.

Source: GAO analysis of DOD information.

[a]FVAP stated that the "Publications" version of the Voting Assistance Guide in PDF format (http://www.fvap.gov/pubs/vag/pdfvag/2006-07vag.pdf) created on October 25, 2005, was the original book version of the Voting Assistance Guide in electronic format. Since it was considered an archived document it was not intended for update.

Appendix III: Comments from the Department of Defense

UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-4000

PERSONNEL AND READINESS

Mr. Derek B. Stewart
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

MAY 23 2007

Dear Mr. Stewart:

This is the Department of Defense (DoD) response to the GAO draft report, 'ELECTIONS: Action Plans Needed to Fully Address Challenges in Electronic Absentee Voting Initiatives for Military and Overseas Citizens,' dated May 9, 2007, (GAO Code 350900/GAO-07-774).

The Department concurs with the recommendations in the report. The Director of the Federal Voting Assistance Program (FVAP) administers the federal provisions of the *Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)* on behalf of the Secretary of Defense. Since 1990, the FVAP has had a proven record of success with electronic alternatives to the by-mail absentee voting process and it continues to coordinate with all major stakeholders in this process, including the state and local level election officials and the U.S. Election Assistance Commission. The Department welcomes input from the GAO and will continue to make improvements to the program in order to better assist citizens covered under the *UOCAVA*.

Thank you for your recommendations and the opportunity to comment on this report.

Sincerely,

David S. C. Chu

Attachment:
1. Comments to the Recommendations

GAO DRAFT REPORT – DATED MAY 9, 2007
GAO CODE 350900/GAO-07-774

"ELECTIONS: Action Plans Needed to Fully Address Challenges in Electronic Absentee Voting Initiatives for Military and Overseas Citizens"

DEPARTMENT OF DEFENSE COMMENTS TO THE RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense direct the Under Secretary of Defense for Personnel and Readiness to comply with the information security requirements in the DoD Certification and Accreditation Process guidance.

DOD RESPONSE: Concur. The Department of Defense will contract for services to comply with the Federal Information Systems Management Act (FISMA) for the Electronic Transmission Service (ETS) through the DoD Information Assurance Certification and Accreditation Process (DIACAP). An extensive set of management, operational and technical controls is currently in place to manage the possible risk to voters and the DoD has begun the process to obtain the necessary certification and accreditation of these controls.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense direct the Under Secretary of Defense for Personnel and Readiness to incorporate lessons learned into plans for future systems such as those we identified including adding cautionary statements to future ballot request and receipt systems to warn Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) voters to remove personal data from their computers.

DOD RESPONSE: Concur. The Department of Defense will incorporate lessons learned for future registration, ballot request and receipt systems, including warnings to remove personal data from computers to guard against voters' personal information being compromised.

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense direct the Under Secretary of Defense for Personnel and Readiness to institutionalize a process to review online Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) guidance to ensure that DoD provides accurate and consistent information to UOCAVA voters.

DOD RESPONSE: Concur. The Federal Voting Assistance Program (FVAP) has already streamlined its online information considerably by eliminating an archived 'Publications' version of the Voting Assistance Guide (VAG) entirely, and by deciding to post only a 'PDF' version of the VAG's State by State instructions for the 2007-2008 VAG. Additionally, the FVAP will also establish a revised review process for online information. These changes will reduce the possibility of human error and simplify the review and verification process of online information.

RECOMMENDATION 4: The GAO recommends that the Secretary of Defense direct the Under Secretary of Defense for Personnel and Readiness to create an integrated, comprehensive, long-term, results-oriented plan for future electronic voting programs that specifies, among other

things, the goals to be achieved along with tasks, milestones, time frames, and contingencies, and synchronizes them with planned development of the Commission's guidelines for Internet voting and safeguards for the security and privacy of all DoD's voting systems – both electronic and Internet. The plan should be developed in conjunction with major stakeholders – including state and local election officials, the Election Assistance Commission, overseas voting groups, and each of the armed services. The plan should also include initiatives that will be done well in advance of Federal elections, to allow adequate time for training and dissemination of information on the options available to Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) voters.

DOD RESPONSE: Concur. The DoD developed and implemented comprehensive plans for Voting Over the Internet and Secure Electronic Registration and Voting Experiment. It is in full support of a long-term, comprehensive plan for future electronic voting projects that would allow for sufficient time to involve the major stakeholders, train and disseminate information and ultimately serve UOCAVA voters. We look forward to working on this multi-year project plan in cooperation with the Election Assistance Commission (EAC), the National Institute of Standards and Technology (NIST) and other major stakeholders. A joint Federal Voting Assistance Program-EAC-NIST meeting is being scheduled to lay the groundwork for "an integrated, comprehensive, long-term, results-oriented plan for future electronic voting programs." We look forward to working with the EAC as they take the lead on the recommended 'action plan' and as we develop our long-term plan in conjunction with them.

Appendix IV: Comments from the Election Assistance Commission

U. S. ELECTION ASSISTANCE COMMISSION
OFFICE OF THE EXECUTIVE DIRECTOR
1225 New York Avenue, NW, Suite 1100
Washington, DC. 20005

May 25, 2007

Mr. Derek B. Stewart
Director, Defense Capabilities
And Management
Government Accountability Office
Washington, DC 20548

RE: Comments regarding proposed GAO-07-774 Report:

Mr. Stewart:

Thank you for the opportunity to comment on the GAO report entitled: *ELECTIONS: Action Plans Needed to Fully Address Challenges in Electronic Absentee Voting Initiatives for Military and Overseas Citizens (GAO-07-774)* submitted to the Election Assistance Commission (EAC) on May 10, 2007. The EAC appreciates GAO's accuracy in its portrayal of the EAC and its current activities regarding military and overseas voters. The EAC is grateful to GAO for its recognition of the EAC's current research efforts to engage election officials and UOCAVA voters prior to the development of these guidelines for military and overseas voters. The EAC also accepts the recommendations as outlined in the report and has begun efforts to achieve the goals as provided to us in the recommendation.

As noted in your report, for the EAC's 2007 research on military and overseas voters, the EAC is conducting the largest survey of UOCAVA voters ever conducted. This survey of ten thousand UOCAVA voters is designed to explore the challenges faced by those voters and determine what solutions have been effective in meeting their unique needs as overseas voters. At last update the EAC had received five thousand replies to the survey and is anticipating more before the data is compiled. As surveys go, this is an excellent response at this point in the process. Based on the replies already received, the EAC is extremely optimistic that the survey results will provide an invaluable look into the UOCAVA experience, and guidance leading to the development of guidelines that are realistic and effective. Also as part of this study, the EAC is conducting case studies of four states that are using new techniques in technology to meet the needs of their UOCAVA voters. The EAC has scheduled a conference to discuss the research results in September of 2007. The EAC will invite election officials, FVAP, NIST, the Overseas Vote Foundation, and other stakeholders to discuss the results of the research and possible solutions to the problems UOCAVA voters face. Also at the conference, the EAC will be conferring with officials from the four states that are participating in the EAC's case studies in order to further explore the unique ways that these states are meeting the demands of their military and overseas voters, and thus help shape the agenda for future guidelines development.

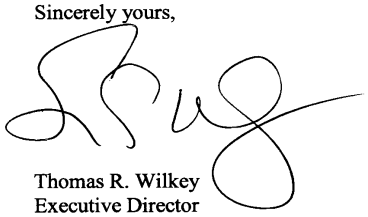
In response to one of the recommendations presented in the report, the EAC would like to note its constant and continued use of election officials in its projects. Besides the election officials who are appointed to the three statutory boards who are regularly updated on EAC projects, the EAC constantly updates election officials throughout the country on research and ongoing projects in order to ensure the work is accurate and useful. The EAC recognizes how important input from these officials is and will continue to work with them, especially those who use creative or new solutions to serve UOCAVA voters.

The EAC would like to reiterate its long held belief that National Institute of Standards and Technology (NIST), because of its internationally recognized technical expertise in developing standards, is essential to the development of voting guidelines for UOCAVA voters. NIST has in the past played a critical role in the development of voting system guidelines. With NIST's guidance the EAC released the newest version of the Voluntary Voting System Guidelines (VVSG) in 2005. Currently NIST is working with the EAC's Technical Guidelines Development Committee to create the next iteration of the VVSG which is a total re-write of VVSG 2005. NIST has consulted FVAP on a several occasions in the past to assist them in regard to UOCAVA voting and the use of the internet.

The EAC has met with FVAP and NIST and reached an agreement to work over the next several months to develop a timeline for the creation of UOCAVA guidelines. We all agree that the release of the EAC's UOCAVA study in September 2007 will be an important first step in this process as it will provide valuable information to help inform the guideline development process. Prior to the release of our study, the EAC, FVAP, and NIST will continue to meet in order to create a reasonable timeline for the creation of the guidelines pursuant to your recommendations.

Again, the EAC would like to thank GAO for the careful analysis of our work in this report and the recommendations to us. The Commission views this issue very seriously and GAO's guidance on this matter is greatly appreciated. We look forward to continued work with FVAP and NIST on this matter and eventually the successful creation of realistic and effective UOCAVA absentee ballot guidelines. Should you have any further questions, please feel free to contact me at (202) 566-3109 or twilkey@eac.gov.

Sincerely yours,



Thomas R. Wilkey
Executive Director

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Derek B. Stewart, (202) 512- 5559 or stewartd@gao.gov

Acknowledgments

In addition to the individual named above, David E. Moser, Assistant Director; Marion A. Gatling; Pawnee A. Davis; Amber M. Lopez; Joanne Landesman; Paula A. Moore; John K. Needham, John J. Smale; and Julia C. Matta made key contributions to this report.

Related GAO Products

Elections: All Levels of Government Are Needed to Address Electronic Voting System Challenges. GAO-07-576T. Washington, D.C.: March 7, 2007.

Elections: DOD Expands Voting Assistance to Military Absentee Voters, but Challenges Remain. GAO-06-1134T. Washington, D.C.: September 28, 2006.

Elections: The Nation's Evolving Election System as Reflected in the November 2004 General Election. GAO-06-450. Washington, D.C.: June 6, 2006.

Election Reform: Nine States' Experiences Implementing Federal Requirements for Computerized Statewide Voter Registration Lists. GAO-06-247. Washington, D.C.: February 7, 2006.

Elections: Views of Selected Local Election Officials on Managing Voter Registration and Ensuring Eligible Citizens Can Vote. GAO-05-997. Washington, D.C.: September 27, 2005.

Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under W ay, but Key Activities Need to Be Completed. GAO-05-956. Washington, D.C.: September 21, 2005.

Elections: Additional Data Could Help State and Local Elections Officials Maintain Accurate Voter Registration Lists. GAO-05-478. Washington, D.C.: June 10, 2005.

Department of Justice's Activities to Address Past Election-Related Voting Irregularities. GAO-04-1041R. Washington, D.C.: September 14, 2004.

Elections: Electronic Voting Offers Opportunities and Presents Challenges. GAO-04-975T. Washington, D.C.: July 20, 2004.

Elections: Voting Assistance to Military and Overseas Citizens Should Be Improved. GAO-01-1026. Washington, D.C.: September 28, 2001.

Elections: The Scope of Congressional Authority in Election Administration. GAO-01-470. Washington, D.C.: March 13, 2001.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

project, we will consider the extent to which the applicant has identified specific gaps and weaknesses in the preparation of all students for postsecondary education and careers without need for remediation, the nature and magnitude of those gaps and weaknesses, and the extent to which the proposed project will address those gaps and weaknesses effectively.

Final Priorities, Requirements, Definition, and Selection Criteria

We will announce the final priorities, requirements, definition, and selection criteria in a notice in the **Federal Register**. We will determine the final priorities, requirements, definitions, and selection criteria after considering responses to this notice and other information available to the Department. This notice does not preclude us from proposing additional priorities, requirements, definitions, and selection criteria, subject to meeting applicable rulemaking requirements.

Note: This notice does not solicit applications. In any year in which we choose to use one or more of these priorities, requirements, definition, and selection criteria, we invite applications through a notice in the **Federal Register.**

Executive Order 12866: This notice has been reviewed in accordance with Executive Order 12866. Under the terms of the order, we have assessed the potential costs and benefits of this regulatory action.

The potential costs associated with this proposed regulatory action are those resulting from statutory requirements and those we have determined as necessary for administering this program effectively and efficiently.

In assessing the potential costs and benefits—both quantitative and qualitative—of this proposed regulatory action, we have determined that the benefits of the proposed priorities, requirements, definition, and selection criteria justify the costs.

We have determined, also, that this regulatory action does not unduly interfere with State, local, and tribal governments in the exercise of their governmental functions.

Discussion of Costs and Benefits: Elsewhere in this notice we discuss the potential costs and benefits, both quantitative and qualitative, of the proposed priorities, requirements, definition, and selection criteria under the background sections to the Priorities, Requirements, Definition, and Selection Criteria.

Paperwork Reduction Act of 1995 (PRA)

Certain sections of the proposed priorities, requirements, definition, and selection criteria for the SLC grant program contain changes to information collection requirements already approved by the Office of Management and Budget (OMB) under OMB control number 1810–0676 (1890–0001). We will be publishing a separate notice in the **Federal Register** requesting comments on these changes.

Intergovernmental Review: This program is subject to Executive Order 12372 and the regulations in 34 CFR part 79. One of the objectives of the Executive order is to foster an intergovernmental partnership and a strengthened federalism. The Executive order relies on processes developed by State and local governments for coordination and review of proposed Federal financial assistance.

This document provides early notification of our specific plans and actions for this program.

Accessible Format: Individuals with disabilities can obtain this document in accessible format (*e.g.,* braille, large print, audiotape, or computer diskette) on request to the program contact person listed under **FOR FURTHER INFORMATION CONTACT**.

Electronic Access to This Document: You can view this document, as well as all other documents of this Department published in the **Federal Register**, in text or Adobe Portable Document Format (PDF) on the Internet at the following site: *http://www.ed.gov/news/fedregister.* To use PDF you must have Adobe Acrobat Reader, which is available free at this site.

Note: The official version of this document is the document published in the **Federal Register**. Free Internet access to the official edition of the **Federal Register** and the Code of Federal Regulations is available on GPO Access at: *http://www.gpoaccess.gov/nara/index.html.*

Dated: March 26, 2010.

Thelma Meléndez de Santa Ana,

Assistant Secretary for Elementary and Secondary Education.

[FR Doc. 2010–7255 Filed 3–30–10; 8:45 am]

BILLING CODE 4000–01–P

ELECTION ASSISTANCE COMMISSION

Proposed Information Quality Guidelines Policy

AGENCY: U.S. Election Assistance Commission (EAC).

ACTION: Notice and request for public comment on Proposed Information Quality Guidelines Policy.

SUMMARY: The U.S. Election Assistance Commission (EAC) seeks public comment on the Proposed Information Quality Guidelines policy. The policy outlines the EAC's directives and required procedures to implement the OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies, 67 FR 8452 ("OMB Guidelines"). The EAC developed the Proposed Information Quality Guidelines to meet its obligations under the OMB Guidelines and to codify its high standards of quality in the production of information disseminated outside the agency.

DATES: Written comments must be submitted on or before 4 p.m. EDT on April 30, 2010.

Comments: Public comments are invited on the information contained in the policy. Comments on the proposed policy should be submitted electronically to *HAVAinfo@eac.gov*. Written comments on the proposed policy can also be sent to the U.S. Election Assistance Commission, 1201 New York Avenue, NW., Suite 300, Washington, DC 20005, ATTN: Proposed Information Quality Guidelines Policy.

Obtaining a Copy of the Policy: To obtain a free copy of the policy: (1) Access the EAC Website at *http://www.eac.gov*; (2) write to the EAC (including your address and phone number) at U.S. Election Assistance Commission, 1201 New York Avenue, NW., Suite 300, Washington, DC 20005, ATTN: Information Quality Guidelines.

FOR FURTHER INFORMATION CONTACT: Ms. Tamar Nedzar, Ms. Karen Lynn-Dyson or Ms. Shelly Anderson at (202) 566–3100.

Thomas R. Wilkey,

Executive Director, U.S. Election Assistance Commission.

[FR Doc. 2010–7134 Filed 3–30–10; 8:45 am]

BILLING CODE 6820–KF–P

ELECTION ASSISTANCE COMMISSION

Notice: Request for Substantive Comments on the EAC's Proposed Requirements for the Testing of Pilot Voting Systems To Serve UOCAVA Voters

AGENCY: United States Election Assistance Commission.

ACTION: Request for public comment on proposed requirements for the testing of

pilot voting systems to be used to serve UOCAVA voters.

SUMMARY: The U.S. Election Assistance Commission (EAC) is publishing for public comment a set of proposed requirements for the testing of pilot voting systems to be used by jurisdictions to serve Uniformed and Overseas voters.

SUPPLEMENTARY INFORMATION:

Background: The Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) of 1986 protects the right to vote in Federal elections for this defined category of citizens. UOCAVA sets out federal and state responsibilities to assist these voters in exercising their voting rights. The Secretary of Defense is the presidential designee responsible for the Federal functions of the Act. The Federal Voting Assistance Program (FVAP) administers this law on behalf of the Secretary of Defense and works cooperatively with other Federal agencies and state and local election officials to carry out its provisions.

UOCAVA legislation was enacted before the advent of today's global electronic communications technology. Consequently it relied on U.S. domestic and military mail systems as well as foreign postal systems for the worldwide distribution of election materials. By the mid-1990s it became apparent that the mail transit time and unreliable delivery posed significant barriers for many UOCAVA citizens, preventing them from successfully exercising their right to vote. At the same time the Internet was being widely adopted by businesses, governments and the general public. Therefore it was a natural development for FVAP and states to consider the potential of the Internet as an alternative to the "by-mail" UOCAVA process.

FVAP sponsored Voting Over the Internet (VOI), a small pilot project for the November 2000 general election, to examine the feasibility of using Internet technology. Four states participated in this experiment, which enabled voters to use their own personal computers to securely register to vote, request and receive absentee ballots, and return their voted ballots. Following the successful completion of the VOI project, in the Fiscal Year 2002 National Defense Authorization Act (section 1604 of Pub. L. 107–107:115 Stat. 1277), Congress instructed the Secretary of Defense to carry out a larger demonstration project for the November 2002 general election. This project was to be "carried out with participation of sufficient numbers of absent uniformed services voters so that the results are statistically significant".

Since there was not sufficient time to define and implement a large project for 2002, the project was planned for implementation for the November 2004 election. Seven states agreed to participate and worked with FVAP to develop system requirements and operating procedures. However, the Secure Electronic Registration and Voting Experiment (SERVE) was cancelled before it was deployed due to concerns raised by several computer scientists. These individuals contended that the use of personal computers over the Internet could not be made secure enough for voting and consequently called for the project to be terminated. The Department of Defense, citing a lack of public confidence in the SERVE system, decided the project could not continue under these circumstances.

In response to this development, the Fiscal Year 2005 National Defense Authorization Act (section 567 of Pub. L. 108–375;118 Stat. 119) repealed the requirement for the Secretary of Defense to conduct an electronic voting demonstration project "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". Pursuant to this legislation, in September 2005, the EAC requested its voting system advisory group, the Technical Guidelines Development Committee (TGDC), to add this subject on their research agenda; however the request was declined.

Since that time legislation dealing with a number of UOCAVA voting issues were under consideration by Congress. Ultimately, passed as part of the Fiscal Year 2010 National Defense Authorization Act (NDAA) (section 581 of Pub. L. 111–84), the Military and Overseas Voters Empowerment Act contains a provision allowing the Secretary of Defense to establish one or more pilot programs to test the feasibility of new election technology for UOCAVA voters. This provision requires the EAC and the National Institute of Standards and Technology (NIST) to provide best practices or standards to support these pilot programs, "in accordance with electronic absentee voting guidelines established under" the earlier FY2005 NDAA. In December 2009, the EAC directed the TGDC to begin this work as a top research priority. The EAC expects this work to result in the comprehensive set of remote electronic voting system guidelines as mandated by the FY2005 NDAA. The TGDC has been tasked to consider the full range of remote voting architectures, including instances where the voter can use his own personal computer for voting. The pilot testing requirements, that the EAC is currently developing, will be provided to the TGDC as the basis and starting point for their research and deliberations.

Project Summary: Since 2008, several states have enacted legislation enabling them to conduct electronic voting projects for UOCAVA voters, beginning with the 2010 elections. To be prepared to support the states with these projects, in July 2009 the EAC convened a UOCAVA Working Group to consider how to adapt the EAC's Testing and Certification Program to accommodate UOCAVA pilot systems. It was concluded that two products were needed: (1) A modified set of system testing requirements; and (2) a revised testing and certification process. It was determined that a working group would assist the EAC in drafting the testing requirements and EAC staff would adapt the certification process to accommodate the UOCAVA pilot program.

The EAC UOCAVA Working Group has taken much the same approach as the state pilot project working groups. The source materials drawn on for this effort included: the Voluntary Voting System Guidelines (VVSG) 1.0 ; the VVSG 1.1; the VVSG 2.0; the VOI, SERVE; FIPS; and NIST Special Publications. One significant difference in the EAC Working Group approach was the technology scope covered by the requirements. The VOI, SERVE and Okaloosa system requirements were tailored specifically for the particular system implementations developed for those projects. However, since many different types of remote voting systems could be submitted to the EAC certification program, the EAC Working Group defined generic system requirements to provide for system design flexibility.

Pilot projects are small in scale and short in duration. Consequently, certification for pilot systems needs to be quicker and less expensive than the regular process currently used for conventional systems with an expected life of more than 10 years. Nevertheless, since actual votes will be cast using the voting systems utilized in the pilot project, the certification process must retain sufficient rigor to provide reasonable assurance that the pilot systems will operate correctly and securely.

There is a fundamental dichotomy in complexity in remote voting architectures: those where the voting

platform is controlled (e.g., provided by the election jurisdiction); and those where it is not controlled (e.g., the voter uses his own personal computer). Since the EAC plans to have the pilot certification process ready for implementation during the first half of 2010, it was decided that the EAC would focus its efforts on controlled platform architectures servicing multiple jurisdictions. This is a highly secure remote voting solution and the Okaloosa Project provides an implementation example for reference. Defining requirements for this class of system architecture was determined to provide a reasonable test case that could be completed within the available timeframe. In addition, most of the core system processing functions are the same for both types of architectures, so a substantial number of requirements will carry over as this work is expanded to include other methods of remote electronic voting.

The UOCAVA Pilot requirements document contains testable requirements for the following areas:

(1) Functional Requirements.
(2) Usability.
(3) Software.
(4) Security.
(5) Quality Assurance.
(6) Configuration Management.
(7) Technical Data Package.
(8) Systems Users Manual.

DATES: Comments must be received on or before 4 p.m. EST on April 15, 2010.

Submission of Comments: The public may submit comments through one of the two different methods provided by the EAC: (1) e-mail submissions to *votingsystemguidelines@eac.gov;* (2) by mail to Voluntary Voting System Guidelines Comments, U.S. Election Assistance Commission, 1201 New York Ave., NW., Suite 300, Washington, DC 20005.

In order to allow efficient and effective review of comments the EAC requests that:

(1) Comments refer to the specific section that is the subject of the comment.

(2) General comments regarding the entire document or comments that refer to more than one section be made as specifically as possible so that EAC can clearly understand to which portion(s) of the documents the comment refers.

(3) To the extent that a comment suggests a change in the wording of a requirement or section of the guidelines, please provide proposed language for the suggested change.

All comments submitted will be published at the end of the comment period on the EAC's Web site at *http://www.eac.gov*. This publication and request for comment is not required under the rulemaking, adjudicative, or licensing provisions of the Administrative Procedures Act (APA). It is a voluntary effort by the EAC to gather input from the public on the EAC's administrative procedures for certifying voting systems to be used in pilot projects. Furthermore, this request by the EAC for public comment is not intended to make any of the APA's rulemaking provisions applicable to development of this or future EAC procedural programs.

An electronic copy of the proposed guidance may be found on the EAC's Web site at *http://www.eac.gov.*

FOR FURTHER INFORMATION CONTACT: Matthew Masterson, Phone (202) 566–3100, e-mail *votingsystemguidelines@eac.gov.*

Alice Miller,

Chief Operating Officer, U.S. Election Assistance Commission.

[FR Doc. 2010–7199 Filed 3–30–10; 8:45 am]

BILLING CODE 6820–KF–P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Project No. 11910–004]

Symbiotics, LLC; AG Hydro, LLC; Notice of Application for Transfer of License, and Soliciting Comments and Motions To Intervene

March 24, 2010.

On March 8, 2010, Symbiotics, LLC (transferor) and AG Hydro, LLC (transferee) filed an application for transfer of license of the Applegate Dam Project, located on the Applegate River in Jackson County, Oregon.

Applicants seek Commission approval to transfer the license for the Applegate Dam from the transferor to the transferee.

Applicant Contact: For both the transferor and transferee is Mr. Brent Smith, 4110 East 300 North, P.O. Box 535, Rigby, ID 83442, phone (208) 745–0834.

FERC Contact: Robert Bell, (202) 502–6062.

Deadline for filing comments and motions to intervene: 30 days from the issuance of this notice. Comments and motions to intervene may be filed electronically via the Internet. See 18 CFR 385.2001(a)(1)(iii)(2008) and the instructions on the Commission's Web site under the "e-Filing" link. If unable to be filed electronically, documents may be paper-filed. To paper-file, an original and eight copies should be mailed to: Kimberly D. Bose, Secretary, Federal Energy Regulatory Commission, 888 First Street, NE., Washington, DC 20426. For more information on how to submit these types of filings please go to the Commission's Web site located at *http://www.ferc.gov/filing-comments.asp.* More information about this project can be viewed or printed on the eLibrary link of the Commission's Web site at *http://www.ferc.gov/docs-filing/elibrary.asp.* Enter the docket number (P–11910–004) in the docket number field to access the document. For assistance, call toll-free 1–866–208–3372.

Kimberly D. Bose,

Secretary.

[FR Doc. 2010–7143 Filed 3–30–10; 8:45 am]

BILLING CODE 6717–01–P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Project No. 1494–384]

Grand River Dam Authority; Notice of Application for Amendment of License and Soliciting Comments, Motions To Intervene, and Protests

March 24, 2010.

Take notice that the following hydroelectric application has been filed with the Commission and is available for public inspection:

a. *Application Type:* Non-project use of project lands and waters.

b. *Project No:* 1494–384.

c. *Date Filed:* March 11, 2010, supplemented on March 17, 2010.

d. *Applicant:* Grand River Dam Authority.

e. *Name of Project:* Pensacola Project.

f. *Location:* The proposed non-project use is located on Grand Lake O' the Cherokees in Delaware County, Oklahoma.

g. *Filed Pursuant to:* Federal Power Act, 16 U.S.C. 791a–825r.

h. *Applicant Contact:* Ms. Tamara E. Jahnke, Assistant General Council, Grand Dam River Authority, P.O. Box 409, Vinita, Oklahoma 74301, (918) 256–5545.

i. *FERC Contact:* Any questions on this notice should be addressed to Shana High at (202) 502–8674.

j. *Deadline for filing comments, motions to intervene, and protest:* April 26, 2010.

Comments, Motions to Intervene, and Protests may be filed electronically via the Internet. See, 18 CFR 385.2001(a)(1)(iii) and the instructions

text or Adobe Portable Document Format (PDF) on the Internet at the following site: *http://www.ed.gov/news/fedregister.* To use PDF you must have Adobe Acrobat Reader, which is available free at this site.

Note: The official version of this document is the document published in the **Federal Register.** Free Internet access to the official edition of the **Federal Register** and the Code of Federal Regulations is available on GPO Access at: *http://www.gpoaccess.gov/nara/index.html.*

Dated: April 6, 2010.

Alexa Posny,

Assistant Secretary for Special Education and Rehabilitative Services.

[FR Doc. 2010–8166 Filed 4–8–10; 8:45 am]

BILLING CODE 4000–01–P

ELECTION ASSISTANCE COMMISSION

Notice: Request for Substantive Comments on the EAC's Procedural Manual for the Election Assistance Commission's Pilot Voting System Testing and Certification Program Manual

AGENCY: United States Election Assistance Commission (EAC).

ACTION: Notice; Request for Substantive Comments.

SUMMARY: The U.S. Election Assistance Commission (EAC) is publishing a procedural manual for its Pilot Voting System Testing and Certification Program Manual for a fifteen day public comment period. This program sets the administrative procedures for manufacturers seeking certification of pilot voting systems to be used in a federal election.

FOR FURTHER INFORMATION CONTACT: Brian Hancock, Director, Voting System Certification, Washington, DC (202) 566–3100, Fax: (202) 566–1392.

SUPPLEMENTARY INFORMATION:

Background. HAVA requires that the EAC certify and decertify voting systems through testing conducted by accredited laboratories. Section 231(a)(1) of HAVA (42 U.S.C. 15371) specifically requires the EAC to "* * * provide for the testing, certification, decertification and recertification of voting system hardware and software by accredited laboratories." To meet this obligation, the EAC has created a voluntary program to test pilot voting systems to a set of voluntary pilot certification requirements. The Pilot Testing Certification Program manual sets the procedures for the pilot voting system manufacturers to follow in order to receive certification for their system to be used in a pilot project for a state or local jurisdiction that require EAC certification.

The Pilot Voting System Testing and Certification program manual contains program requirements and procedures for the following areas:

1. Voting system manufacturer registration.
2. When voting system intended for use in a pilot must be submitted for certification.
3. Certification Testing, Technical Review and Grant of Certification for Pilot Voting Systems.
4. Denial of Certification.
5. Pilot Program Monitoring and Reporting.
6. Requests for Interpretations.
7. Release of Certification Program Information.

Substantive Comments: The EAC seeks substantive comments from the public on its proposed procedural manual. Please submit comments consistent with the information below. Comments should identify and cite the section of the manual at issue. Where a substantive issue is raised, please propose a recommended change or alternative policy. All comments submitted will be published at the end of the comment period on the EAC's Web site at *http://www.eac.gov*. This publication and request for comment is not required under the rulemaking, adjudicative, or licensing provisions of the Administrative Procedures Act (APA). It is a voluntary effort by the EAC to gather input from the public on the EAC's administrative procedures for certifying voting systems to be used in pilot projects. Furthermore, this request by the EAC for public comment is not intended to make any of the APA's rulemaking provisions applicable to development of this or future EAC procedural programs. However, in accordance with the Paperwork Reduction Act of 1995, a separate notice will be published on the **Federal Register** to request comments regarding the burden of responding to the information collection activities of the proposed manual; please refer to the EAC's Web site, *http://www.eac.gov*, for further information about the submission of comments regarding burden.

DATES: Submit written or electronic comments on this draft procedural manual on or before 5 p.m. EDT on April 26, 2010.

ADDRESSES: Submit comments via e-mail to *votingsystemguidelines@eac.gov;* via mail to Brian Hancock, Director of Voting System Certification, U.S. Election Assistance Commission, 1201 New York Avenue, Suite 300, Washington, DC 20005; or via fax to 202–566–1392. An electronic copy of the proposed guidance may be found on the EAC's Web site at *http://www.eac.gov.*

FOR FURTHER INFORMATION CONTACT: Matthew Masterson, Deputy Director, Testing and Certification Program 1201 New York Avenue, Suite 300, Washington, DC, (202) 566–3100, *Fax:* (202) 566–1392.

Alice Miller,

Chief Operating Officer, U.S. Election Assistance Commission.

[FR Doc. 2010–8150 Filed 4–8–10; 8:45 am]

BILLING CODE 6820–KF–P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Project No. 13655–000]

Riverbank Minnesota, LLC; Notice of Preliminary Permit Application Accepted for Filing and Soliciting Comments, Motions To Intervene, and Competing Applications

April 2, 2010.

On January 12, 2010, Riverbank Minnesota, LLC filed an application, pursuant to section 4(f) of the Federal Power Act, proposing to study the feasibility of the Granite Falls Pumped Storage Project No. 13655, to be located east of the City of Granite Falls and the Minnesota River in Chippewa County, Minnesota.

The proposed pumped storage project would consist of: (1) A new approximately 135-acre, 30-foot-deep upper reservoir constructed of enclosed earth embankments; (2) a new lower reservoir excavated in granite bedrock at a depth of approximately 1,800 feet below the surface, consisting of six approximately 150-foot-high, 90-foot-wide underground galleries; (3) a new approximately 20 to 100-foot-diameter intake structure; (4) a new approximately 1,800-foot-long, 20-foot-diameter penstock from the intake structure to an underground powerhouse; (5) a new approximately 380-foot-long, 83-foot-wide, and 400-foot-high underground powerhouse; (6) four new reversible pump-turbines with a total combined capacity of 1,000 megawatts; (7) a new 330-foot-long, 55-foot-wide, and 400-foot-high transformer gallery; (8) a new approximately 1.2-mile-long, 230-kilovolt transmission line; and (9) appurtenant facilities. The project

ZUCKERMAN SPAEDER LLP

Eleanor H. Smith
(202) 778-1838
esmith@zuckerman.com

1800 M Street NW Ste 1000
Washington, D.C. 20036
(202) 822-8106 (facsimile)

April 15, 2010

VIA E-MAIL (votingsystemguidelines@eac.gov) and (ddavidson@eac.gov) & HAND DELIVERY

U.S. Election Assistance Commission
c/o Donetta Davidson, Chair
1201 New York Avenue, NW, Ste 300
Washington, D.C. 20005

Re: EAC Violation of the Administrative Procedure Act Regarding Proposed Requirements for Federal Certification of Voting Systems for U.S. Uniformed and Overseas Citizens to Vote in the 2010 Election

Dear Commissioners:

This letter responds to denial by the Election Assistance Commission of a request I made April 13, 2010 on behalf of Voter Action, and others who may join its comments, for an extension of time to comment on recently published proposed requirements. These EAC requirements would govern federal certification of voting systems to be used by United States citizens in the uniformed services or located overseas, to vote in the 2010 elections for the U.S. Senate, the U.S. House of Representatives, and state and local elected offices. A copy of the denial letter is attached at Tab A.

Voter Action is a national non-profit organization that seeks to ensure election integrity in the United States. Voter Action aims to protect an open and transparent election process, one in which our elections at the federal, state, and local level are accessible and verifiable. Voter Action supports the basic civil and political rights of all voters to cast their ballots in an independent manner and to have to their votes accurately recorded and counted.

As you are aware, the EAC published a "Request for Substantive Comments on the EAC's Proposed Requirements for the Testing of Pilot Voting Systems To Serve UOCAVA Voters" in the *Federal Register* on March 31, 2010, setting a deadline for public comments of "before 4 p.m. EST on April 15, 2010." *See* 61 Fed. Reg. 16088-90 (Mar. 31, 2010) (attached at Tab B). In addition, the EAC has published a "Request for Substantive Comments on the EAC's Procedural Manual for the Election Assistance Commission's Pilot Voting System Testing and Certification Program Manual" in the *Federal Register* on April 9, 2010, setting a deadline for public comments of "before 5 p.m.

EDT on April 26, 2010." *See* 61 Fed. Reg. 18189 (Apr. 9, 2010) (Attached at Tab C). These notices erroneously disavow the notice and comment requirements of the Administrative Procedure Act (APA), 5 U.S.C.§ 551 *et seq*, and provide a mere 15 days for "substantive comments" regarding requirements that would impact the substantive rights of eligible U.S. voters to vote and have their vote counted as cast.

Fifteen days notice simply is not adequate to permit the public to comment on the proposed requirements and implementing manual to govern voting systems to be used by U.S. citizens in uniform or living abroad to vote on voting systems involving the internet – something that would be sanctioned by the EAC for the first time. Executive Order 12866, which helps to implement the APA, provides that "each agency should afford the public a meaningful opportunity to comment on any proposed regulation, which in most cases should include a ***comment period of not less than 60 days***." Exec. Order No. 12866, § 6(a)(1) (Sep. 30, 1993) (emphases added) (Attached at Tab D). One of the stated objectives of Executive Order 12866 is "to make the [regulatory] process more accessible and open to the public." Regrettably the EAC's notice, allowing only one-fourth of the 60 day time period established by Executive Order 12866, accomplishes precisely the opposite. Indeed, the short time period set by the EAC to comment on the proposed internet voting system requirements and manual ensures that few persons will be aware of the comment period, much less have time to prepare and submit comments before the comment period ends. If anything, one would expect the EAC to provide *more* than 60 days notice to accommodate the comments of those concerned about whether these proposed requirements and related manual protect each person's vote and the likelihood of a lag time in notification to those living abroad, including the brave men and women in our Armed Forces who are busy fighting wars on foreign soil on our behalf.

There are facts that make the notice period selected by the EAC even more troublesome. April 15, 2010 is the day before computer scientists who specialize in trustworthy elections have to submit their work product for the 2010 Electronic Voting Technology Workshop/Workshop on Trustworthy Election (EVT/WOTE '10). A copy of a webpage regarding this electronic voting technology workshop is attached at Tab E. April 15, 2010, also is the date by which income tax returns in the United States must be filed. This is a time when people are acutely distracted by other demands, making them much less likely to focus on what the EAC is doing. Moreover, the denial by the EAC of an extension of time to comment purports to preclude the acceptance of comments on the voting system testing and certification requirements after April 15, 2010, even though the comment period for the related voting system testing and certification manual remains open for another 11 days, until April 26, 2010.

The EAC is requested to notify the public within the next week that it is extending for at least 45 more days beyond April 26, 2010, the period of comment upon the proposed requirements (and

related manual) for federal certification of voting systems for use by uniformed and overseas voters to vote in the 2010 U.S. election.

Sincerely,

Eleanor H. Smith

Enclosures

cc: Gracia Hillman, Commissioner
Gineen Bresso Beach, Commissioner
Thomas R. Wilkey, Executive Director
Juliet E. Thompson, General Counsel
Sarah Litton, Deputy Director of Communications (Email- slitton@eac.gov and U.S. Mail)
John C. Bonifaz, Voter Action, Legal Director (Email- jbonifaz@voteraction.org and U.S. Mail)

TAB
A

Smith, Eleanor H.

From: slitton@eac.gov
Sent: Wednesday, April 14, 2010 8:54 AM
To: Smith, Eleanor H.
Subject: EAC Comment Period

Ms. Smith,

Please submit any comments about the UOCAVA Pilot Program Testing Requirements by the stated deadline of April 15. The timeline for the pilot program, including the comment periods, was established to reach a goal of having a set of testable requirements for pilot systems to possibly be used by jurisdictions in the 2010 general election. As a reminder, the Pilot Program Testing Requirements will only be used for pilot projects during the 2010 election cycle. We will be holding a comment period for at least 90 days for the next iteration of the VVSG later this year, and hope you will also be able to share your comments during that process.

Sarah Litton
Deputy Director of Communications
U.S. Election Assistance Commission
1225 New York Avenue, NW, Suite 1100
Washington, DC 20005
www.eac.gov
(202) 566-3100

TAB
B

project, we will consider the extent to which the applicant has identified specific gaps and weaknesses in the preparation of all students for postsecondary education and careers without need for remediation, the nature and magnitude of those gaps and weaknesses, and the extent to which the proposed project will address those gaps and weaknesses effectively.

Final Priorities, Requirements, Definition, and Selection Criteria

We will announce the final priorities, requirements, definition, and selection criteria in a notice in the **Federal Register**. We will determine the final priorities, requirements, definitions, and selection criteria after considering responses to this notice and other information available to the Department. This notice does not preclude us from proposing additional priorities, requirements, definitions, and selection criteria, subject to meeting applicable rulemaking requirements.

Note: This notice does not solicit applications. In any year in which we choose to use one or more of these priorities, requirements, definition, and selection criteria, we invite applications through a notice in the **Federal Register.**

Executive Order 12866: This notice has been reviewed in accordance with Executive Order 12866. Under the terms of the order, we have assessed the potential costs and benefits of this regulatory action.

The potential costs associated with this proposed regulatory action are those resulting from statutory requirements and those we have determined as necessary for administering this program effectively and efficiently.

In assessing the potential costs and benefits—both quantitative and qualitative—of this proposed regulatory action, we have determined that the benefits of the proposed priorities, requirements, definition, and selection criteria justify the costs.

We have determined, also, that this regulatory action does not unduly interfere with State, local, and tribal governments in the exercise of their governmental functions.

Discussion of Costs and Benefits: Elsewhere in this notice we discuss the potential costs and benefits, both quantitative and qualitative, of the proposed priorities, requirements, definition, and selection criteria under the background sections to the Priorities, Requirements, Definition, and Selection Criteria.

Paperwork Reduction Act of 1995 (PRA)

Certain sections of the proposed priorities, requirements, definition, and selection criteria for the SLC grant program contain changes to information collection requirements already approved by the Office of Management and Budget (OMB) under OMB control number 1810–0676 (1890–0001). We will be publishing a separate notice in the **Federal Register** requesting comments on these changes.

Intergovernmental Review: This program is subject to Executive Order 12372 and the regulations in 34 CFR part 79. One of the objectives of the Executive order is to foster an intergovernmental partnership and a strengthened federalism. The Executive order relies on processes developed by State and local governments for coordination and review of proposed Federal financial assistance.

This document provides early notification of our specific plans and actions for this program.

Accessible Format: Individuals with disabilities can obtain this document in accessible format (*e.g.*, braille, large print, audiotape, or computer diskette) on request to the program contact person listed under **FOR FURTHER INFORMATION CONTACT.**

Electronic Access to This Document: You can view this document, as well as all other documents of this Department published in the **Federal Register**, in text or Adobe Portable Document Format (PDF) on the Internet at the following site: *http://www.ed.gov/news/fedregister.* To use PDF you must have Adobe Acrobat Reader, which is available free at this site.

Note: The official version of this document is the document published in the **Federal Register.** Free Internet access to the official edition of the **Federal Register** and the Code of Federal Regulations is available on GPO Access at: *http://www.gpoaccess.gov/nara/index.html.*

Dated: March 26, 2010.

Thelma Meléndez de Santa Ana,

Assistant Secretary for Elementary and Secondary Education.

[FR Doc. 2010–7255 Filed 3–30–10; 8:45 am]

BILLING CODE 4000–01–P

ELECTION ASSISTANCE COMMISSION

Proposed Information Quality Guidelines Policy

AGENCY: U.S. Election Assistance Commission (EAC).

ACTION: Notice and request for public comment on Proposed Information Quality Guidelines Policy.

SUMMARY: The U.S. Election Assistance Commission (EAC) seeks public comment on the Proposed Information Quality Guidelines policy. The policy outlines the EAC's directives and required procedures to implement the OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies, 67 FR 8452 ("OMB Guidelines"). The EAC developed the Proposed Information Quality Guidelines to meet its obligations under the OMB Guidelines and to codify its high standards of quality in the production of information disseminated outside the agency.

DATES: Written comments must be submitted on or before 4 p.m. EDT on April 30, 2010.

Comments: Public comments are invited on the information contained in the policy. Comments on the proposed policy should be submitted electronically to *HAVAinfo@eac.gov.* Written comments on the proposed policy can also be sent to the U.S. Election Assistance Commission, 1201 New York Avenue, NW., Suite 300, Washington, DC 20005, ATTN: Proposed Information Quality Guidelines Policy.

Obtaining a Copy of the Policy: To obtain a free copy of the policy: (1) Access the EAC Website at *http://www.eac.gov*; (2) write to the EAC (including your address and phone number) at U.S. Election Assistance Commission, 1201 New York Avenue, NW., Suite 300, Washington, DC 20005, ATTN: Information Quality Guidelines.

FOR FURTHER INFORMATION CONTACT: Ms. Tamar Nedzar, Ms. Karen Lynn-Dyson or Ms. Shelly Anderson at (202) 566–3100.

Thomas R. Wilkey,

Executive Director, U.S. Election Assistance Commission.

[FR Doc. 2010–7134 Filed 3–30–10; 8:45 am]

BILLING CODE 6820–KF–P

ELECTION ASSISTANCE COMMISSION

Notice: Request for Substantive Comments on the EAC's Proposed Requirements for the Testing of Pilot Voting Systems To Serve UOCAVA Voters

AGENCY: United States Election Assistance Commission.

ACTION: Request for public comment on proposed requirements for the testing of

pilot voting systems to be used to serve UOCAVA voters.

SUMMARY: The U.S. Election Assistance Commission (EAC) is publishing for public comment a set of proposed requirements for the testing of pilot voting systems to be used by jurisdictions to serve Uniformed and Overseas voters.

SUPPLEMENTARY INFORMATION:

Background: The Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) of 1986 protects the right to vote in Federal elections for this defined category of citizens. UOCAVA sets out federal and state responsibilities to assist these voters in exercising their voting rights. The Secretary of Defense is the presidential designee responsible for the Federal functions of the Act. The Federal Voting Assistance Program (FVAP) administers this law on behalf of the Secretary of Defense and works cooperatively with other Federal agencies and state and local election officials to carry out its provisions.

UOCAVA legislation was enacted before the advent of today's global electronic communications technology. Consequently it relied on U.S. domestic and military mail systems as well as foreign postal systems for the worldwide distribution of election materials. By the mid-1990s it became apparent that the mail transit time and unreliable delivery posed significant barriers for many UOCAVA citizens, preventing them from successfully exercising their right to vote. At the same time the Internet was being widely adopted by businesses, governments and the general public. Therefore it was a natural development for FVAP and states to consider the potential of the Internet as an alternative to the "by-mail" UOCAVA process.

FVAP sponsored Voting Over the Internet (VOI), a small pilot project for the November 2000 general election, to examine the feasibility of using Internet technology. Four states participated in this experiment, which enabled voters to use their own personal computers to securely register to vote, request and receive absentee ballots, and return their voted ballots. Following the successful completion of the VOI project, in the Fiscal Year 2002 National Defense Authorization Act (section 1604 of Pub. L. 107–107:115 Stat. 1277), Congress instructed the Secretary of Defense to carry out a larger demonstration project for the November 2002 general election. This project was to be "carried out with participation of sufficient numbers of absent uniformed services voters so that the results are statistically significant".

Since there was not sufficient time to define and implement a large project for 2002, the project was planned for implementation for the November 2004 election. Seven states agreed to participate and worked with FVAP to develop system requirements and operating procedures. However, the Secure Electronic Registration and Voting Experiment (SERVE) was cancelled before it was deployed due to concerns raised by several computer scientists. These individuals contended that the use of personal computers over the Internet could not be made secure enough for voting and consequently called for the project to be terminated. The Department of Defense, citing a lack of public confidence in the SERVE system, decided the project could not continue under these circumstances.

In response to this development, the Fiscal Year 2005 National Defense Authorization Act (section 567 of Pub. L. 108–375;118 Stat. 119) repealed the requirement for the Secretary of Defense to conduct an electronic voting demonstration project "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". Pursuant to this legislation, in September 2005, the EAC requested its voting system advisory group, the Technical Guidelines Development Committee (TGDC), to add this subject on their research agenda; however the request was declined.

Since that time legislation dealing with a number of UOCAVA voting issues were under consideration by Congress. Ultimately, passed as part of the Fiscal Year 2010 National Defense Authorization Act (NDAA) (section 581 of Pub. L. 111–84), the Military and Overseas Voters Empowerment Act contains a provision allowing the Secretary of Defense to establish one or more pilot programs to test the feasibility of new election technology for UOCAVA voters. This provision requires the EAC and the National Institute of Standards and Technology (NIST) to provide best practices or standards to support these pilot programs, "in accordance with electronic absentee voting guidelines established under" the earlier FY2005 NDAA. In December 2009, the EAC directed the TGDC to begin this work as a top research priority. The EAC expects this work to result in the comprehensive set of remote electronic voting system guidelines as mandated by the FY2005 NDAA. The TGDC has been tasked to consider the full range of remote voting architectures, including instances where the voter can use his own personal computer for voting. The pilot testing requirements, that the EAC is currently developing, will be provided to the TGDC as the basis and starting point for their research and deliberations.

Project Summary: Since 2008, several states have enacted legislation enabling them to conduct electronic voting projects for UOCAVA voters, beginning with the 2010 elections. To be prepared to support the states with these projects, in July 2009 the EAC convened a UOCAVA Working Group to consider how to adapt the EAC's Testing and Certification Program to accommodate UOCAVA pilot systems. It was concluded that two products were needed: (1) A modified set of system testing requirements; and (2) a revised testing and certification process. It was determined that a working group would assist the EAC in drafting the testing requirements and EAC staff would adapt the certification process to accommodate the UOCAVA pilot program.

The EAC UOCAVA Working Group has taken much the same approach as the state pilot project working groups. The source materials drawn on for this effort included: the Voluntary Voting System Guidelines (VVSG) 1.0 ; the VVSG 1.1; the VVSG 2.0; the VOI, SERVE; FIPS; and NIST Special Publications. One significant difference in the EAC Working Group approach was the technology scope covered by the requirements. The VOI, SERVE and Okaloosa system requirements were tailored specifically for the particular system implementations developed for those projects. However, since many different types of remote voting systems could be submitted to the EAC certification program, the EAC Working Group defined generic system requirements to provide for system design flexibility.

Pilot projects are small in scale and short in duration. Consequently, certification for pilot systems needs to be quicker and less expensive than the regular process currently used for conventional systems with an expected life of more than 10 years. Nevertheless, since actual votes will be cast using the voting systems utilized in the pilot project, the certification process must retain sufficient rigor to provide reasonable assurance that the pilot systems will operate correctly and securely.

There is a fundamental dichotomy in complexity in remote voting architectures: those where the voting

platform is controlled (e.g., provided by the election jurisdiction); and those where it is not controlled (e.g., the voter uses his own personal computer). Since the EAC plans to have the pilot certification process ready for implementation during the first half of 2010, it was decided that the EAC would focus its efforts on controlled platform architectures servicing multiple jurisdictions. This is a highly secure remote voting solution and the Okaloosa Project provides an implementation example for reference. Defining requirements for this class of system architecture was determined to provide a reasonable test case that could be completed within the available timeframe. In addition, most of the core system processing functions are the same for both types of architectures, so a substantial number of requirements will carry over as this work is expanded to include other methods of remote electronic voting.

The UOCAVA Pilot requirements document contains testable requirements for the following areas:

(1) Functional Requirements.
(2) Usability.
(3) Software.
(4) Security.
(5) Quality Assurance.
(6) Configuration Management.
(7) Technical Data Package.
(8) Systems Users Manual.

DATES: Comments must be received on or before 4 p.m. EST on April 15, 2010.

Submission of Comments: The public may submit comments through one of the two different methods provided by the EAC: (1) e-mail submissions to *votingsystemguidelines@eac.gov;* (2) by mail to Voluntary Voting System Guidelines Comments, U.S. Election Assistance Commission, 1201 New York Ave., NW., Suite 300, Washington, DC 20005.

In order to allow efficient and effective review of comments the EAC requests that:

(1) Comments refer to the specific section that is the subject of the comment.

(2) General comments regarding the entire document or comments that refer to more than one section be made as specifically as possible so that EAC can clearly understand to which portion(s) of the documents the comment refers.

(3) To the extent that a comment suggests a change in the wording of a requirement or section of the guidelines, please provide proposed language for the suggested change.

All comments submitted will be published at the end of the comment period on the EAC's Web site at *http://www.eac.gov.* This publication and request for comment is not required under the rulemaking, adjudicative, or licensing provisions of the Administrative Procedures Act (APA). It is a voluntary effort by the EAC to gather input from the public on the EAC's administrative procedures for certifying voting systems to be used in pilot projects. Furthermore, this request by the EAC for public comment is not intended to make any of the APA's rulemaking provisions applicable to development of this or future EAC procedural programs.

An electronic copy of the proposed guidance may be found on the EAC's Web site at *http://www.eac.gov.*

FOR FURTHER INFORMATION CONTACT: Matthew Masterson, Phone (202) 566–3100, e-mail *votingsystemguidelines@eac.gov.*

Alice Miller,

Chief Operating Officer, U.S. Election Assistance Commission.

[FR Doc. 2010–7199 Filed 3–30–10; 8:45 am]

BILLING CODE 6820–KF–P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Project No. 11910–004]

Symbiotics, LLC; AG Hydro, LLC; Notice of Application for Transfer of License, and Soliciting Comments and Motions To Intervene

March 24, 2010.

On March 8, 2010, Symbiotics, LLC (transferor) and AG Hydro, LLC (transferee) filed an application for transfer of license of the Applegate Dam Project, located on the Applegate River in Jackson County, Oregon.

Applicants seek Commission approval to transfer the license for the Applegate Dam from the transferor to the transferee.

Applicant Contact: For both the transferor and transferee is Mr. Brent Smith, 4110 East 300 North, P.O. Box 535, Rigby, ID 83442, phone (208) 745–0834.

FERC Contact: Robert Bell, (202) 502–6062.

Deadline for filing comments and motions to intervene: 30 days from the issuance of this notice. Comments and motions to intervene may be filed electronically via the Internet. See 18 CFR 385.2001(a)(1)(iii)(2008) and the instructions on the Commission's Web site under the "e-Filing" link. If unable to be filed electronically, documents may be paper-filed. To paper-file, an original and eight copies should be mailed to: Kimberly D. Bose, Secretary, Federal Energy Regulatory Commission, 888 First Street, NE., Washington, DC 20426. For more information on how to submit these types of filings please go to the Commission's Web site located at *http://www.ferc.gov/filing-comments.asp.* More information about this project can be viewed or printed on the eLibrary link of the Commission's Web site at *http://www.ferc.gov/docs-filing/elibrary.asp.* Enter the docket number (P–11910–004) in the docket number field to access the document. For assistance, call toll-free 1–866–208–3372.

Kimberly D. Bose,

Secretary.

[FR Doc. 2010–7143 Filed 3–30–10; 8:45 am]

BILLING CODE 6717–01–P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Project No. 1494–384]

Grand River Dam Authority; Notice of Application for Amendment of License and Soliciting Comments, Motions To Intervene, and Protests

March 24, 2010.

Take notice that the following hydroelectric application has been filed with the Commission and is available for public inspection:

a. *Application Type:* Non-project use of project lands and waters.

b. *Project No:* 1494–384.

c. *Date Filed:* March 11, 2010, supplemented on March 17, 2010.

d. *Applicant:* Grand River Dam Authority.

e. *Name of Project:* Pensacola Project.

f. *Location:* The proposed non-project use is located on Grand Lake O' the Cherokees in Delaware County, Oklahoma.

g. *Filed Pursuant to:* Federal Power Act, 16 U.S.C. 791a–825r.

h. *Applicant Contact:* Ms. Tamara E. Jahnke, Assistant General Council, Grand Dam River Authority, P.O. Box 409, Vinita, Oklahoma 74301, (918) 256–5545.

i. *FERC Contact:* Any questions on this notice should be addressed to Shana High at (202) 502–8674.

j. *Deadline for filing comments, motions to intervene, and protest:* April 26, 2010.

Comments, Motions to Intervene, and Protests may be filed electronically via the Internet. See, 18 CFR 385.2001(a)(1)(iii) and the instructions

TAB
C

text or Adobe Portable Document Format (PDF) on the Internet at the following site: *http://www.ed.gov/news/fedregister*. To use PDF you must have Adobe Acrobat Reader, which is available free at this site.

Note: The official version of this document is the document published in the **Federal Register**. Free Internet access to the official edition of the **Federal Register** and the Code of Federal Regulations is available on GPO Access at: *http://www.gpoaccess.gov/nara/index.html*.

Dated: April 6, 2010.

Alexa Posny,

Assistant Secretary for Special Education and Rehabilitative Services.

[FR Doc. 2010–8166 Filed 4–8–10; 8:45 am]

BILLING CODE 4000–01–P

ELECTION ASSISTANCE COMMISSION

Notice: Request for Substantive Comments on the EAC's Procedural Manual for the Election Assistance Commission's Pilot Voting System Testing and Certification Program Manual

AGENCY: United States Election Assistance Commission (EAC).

ACTION: Notice; Request for Substantive Comments.

SUMMARY: The U.S. Election Assistance Commission (EAC) is publishing a procedural manual for its Pilot Voting System Testing and Certification Program Manual for a fifteen day public comment period. This program sets the administrative procedures for manufacturers seeking certification of pilot voting systems to be used in a federal election.

FOR FURTHER INFORMATION CONTACT: Brian Hancock, Director, Voting System Certification, Washington, DC (202) 566–3100, Fax: (202) 566–1392.

SUPPLEMENTARY INFORMATION:

Background. HAVA requires that the EAC certify and decertify voting systems through testing conducted by accredited laboratories. Section 231(a)(1) of HAVA (42 U.S.C. 15371) specifically requires the EAC to "* * * provide for the testing, certification, decertification and recertification of voting system hardware and software by accredited laboratories." To meet this obligation, the EAC has created a voluntary program to test pilot voting systems to a set of voluntary pilot certification requirements. The Pilot Testing Certification Program manual sets the procedures for the pilot voting system manufacturers to follow in order to receive certification for their system to be used in a pilot project for a state or local jurisdiction that require EAC certification.

The Pilot Voting System Testing and Certification program manual contains program requirements and procedures for the following areas:

1. Voting system manufacturer registration.
2. When voting system intended for use in a pilot must be submitted for certification.
3. Certification Testing, Technical Review and Grant of Certification for Pilot Voting Systems.
4. Denial of Certification.
5. Pilot Program Monitoring and Reporting.
6. Requests for Interpretations.
7. Release of Certification Program Information.

Substantive Comments: The EAC seeks substantive comments from the public on its proposed procedural manual. Please submit comments consistent with the information below. Comments should identify and cite the section of the manual at issue. Where a substantive issue is raised, please propose a recommended change or alternative policy. All comments submitted will be published at the end of the comment period on the EAC's Web site at *http://www.eac.gov*. This publication and request for comment is not required under the rulemaking, adjudicative, or licensing provisions of the Administrative Procedures Act (APA). It is a voluntary effort by the EAC to gather input from the public on the EAC's administrative procedures for certifying voting systems to be used in pilot projects. Furthermore, this request by the EAC for public comment is not intended to make any of the APA's rulemaking provisions applicable to development of this or future EAC procedural programs. However, in accordance with the Paperwork Reduction Act of 1995, a separate notice will be published on the **Federal Register** to request comments regarding the burden of responding to the information collection activities of the proposed manual; please refer to the EAC's Web site, *http://www.eac.gov*, for further information about the submission of comments regarding burden.

DATES: Submit written or electronic comments on this draft procedural manual on or before 5 p.m. EDT on April 26, 2010.

ADDRESSES: Submit comments via e-mail to *votingsystemguidelines@eac.gov;* via mail to Brian Hancock, Director of Voting System Certification, U.S. Election Assistance Commission, 1201 New York Avenue, Suite 300, Washington, DC 20005; or via fax to 202–566–1392. An electronic copy of the proposed guidance may be found on the EAC's Web site at *http://www.eac.gov*.

FOR FURTHER INFORMATION CONTACT: Matthew Masterson, Deputy Director, Testing and Certification Program 1201 New York Avenue, Suite 300, Washington, DC, (202) 566–3100, *Fax:* (202) 566–1392.

Alice Miller,

Chief Operating Officer, U.S. Election Assistance Commission.

[FR Doc. 2010–8150 Filed 4–8–10; 8:45 am]

BILLING CODE 6820–KF–P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Project No. 13655–000]

Riverbank Minnesota, LLC; Notice of Preliminary Permit Application Accepted for Filing and Soliciting Comments, Motions To Intervene, and Competing Applications

April 2, 2010.

On January 12, 2010, Riverbank Minnesota, LLC filed an application, pursuant to section 4(f) of the Federal Power Act, proposing to study the feasibility of the Granite Falls Pumped Storage Project No. 13655, to be located east of the City of Granite Falls and the Minnesota River in Chippewa County, Minnesota.

The proposed pumped storage project would consist of: (1) A new approximately 135-acre, 30-foot-deep upper reservoir constructed of enclosed earth embankments; (2) a new lower reservoir excavated in granite bedrock at a depth of approximately 1,800 feet below the surface, consisting of six approximately 150-foot-high, 90-foot-wide underground galleries; (3) a new approximately 20 to 100-foot-diameter intake structure; (4) a new approximately 1,800-foot-long, 20-foot-diameter penstock from the intake structure to an underground powerhouse; (5) a new approximately 380-foot-long, 83-foot-wide, and 400-foot-high underground powerhouse; (6) four new reversible pump-turbines with a total combined capacity of 1,000 megawatts; (7) a new 330-foot-long, 55-foot-wide, and 400-foot-high transformer gallery; (8) a new approximately 1.2-mile-long, 230-kilovolt transmission line; and (9) appurtenant facilities. The project

TAB
D

federal register

Monday
October 4, 1993

Part VIII

The President

Executive Order 12866—Regulatory Planning and Review

Federal Register
Vol. 58, No. 190
Monday, October 4, 1993

Presidential Documents

Title 3—

The President

Executive Order 12866 of September 30, 1993

Regulatory Planning and Review

The American people deserve a regulatory system that works for them, not against them: a regulatory system that protects and improves their health, safety, environment, and well-being and improves the performance of the economy without imposing unacceptable or unreasonable costs on society; regulatory policies that recognize that the private sector and private markets are the best engine for economic growth; regulatory approaches that respect the role of State, local, and tribal governments; and regulations that are effective, consistent, sensible, and understandable. We do not have such a regulatory system today.

With this Executive order, the Federal Government begins a program to reform and make more efficient the regulatory process. The objectives of this Executive order are to enhance planning and coordination with respect to both new and existing regulations; to reaffirm the primacy of Federal agencies in the regulatory decision-making process; to restore the integrity and legitimacy of regulatory review and oversight; and to make the process more accessible and open to the public. In pursuing these objectives, the regulatory process shall be conducted so as to meet applicable statutory requirements and with due regard to the discretion that has been entrusted to the Federal agencies.

Accordingly, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Statement of Regulatory Philosophy and Principles.* (a) *The Regulatory Philosophy.* Federal agencies should promulgate only such regulations as are required by law, are necessary to interpret the law, or are made necessary by compelling public need, such as material failures of private markets to protect or improve the health and safety of the public, the environment, or the well-being of the American people. In deciding whether and how to regulate, agencies should assess all costs and benefits of available regulatory alternatives, including the alternative of not regulating. Costs and benefits shall be understood to include both quantifiable measures (to the fullest extent that these can be usefully estimated) and qualitative measures of costs and benefits that are difficult to quantify, but nevertheless essential to consider. Further, in choosing among alternative regulatory approaches, agencies should select those approaches that maximize net benefits (including potential economic, environmental, public health and safety, and other advantages; distributive impacts; and equity), unless a statute requires another regulatory approach.

(b) *The Principles of Regulation.* To ensure that the agencies' regulatory programs are consistent with the philosophy set forth above, agencies should adhere to the following principles, to the extent permitted by law and where applicable:

(1) Each agency shall identify the problem that it intends to address (including, where applicable, the failures of private markets or public institutions that warrant new agency action) as well as assess the significance of that problem.

(2) Each agency shall examine whether existing regulations (or other law) have created, or contributed to, the problem that a new regulation

is intended to correct and whether those regulations (or other law) should be modified to achieve the intended goal of regulation more effectively.

(3) Each agency shall identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, such as user fees or marketable permits, or providing information upon which choices can be made by the public.

(4) In setting regulatory priorities, each agency shall consider, to the extent reasonable, the degree and nature of the risks posed by various substances or activities within its jurisdiction.

(5) When an agency determines that a regulation is the best available method of achieving the regulatory objective, it shall design its regulations in the most cost-effective manner to achieve the regulatory objective. In doing so, each agency shall consider incentives for innovation, consistency, predictability, the costs of enforcement and compliance (to the government, regulated entities, and the public), flexibility, distributive impacts, and equity.

(6) Each agency shall assess both the costs and the benefits of the intended regulation and, recognizing that some costs and benefits are difficult to quantify, propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs.

(7) Each agency shall base its decisions on the best reasonably obtainable scientific, technical, economic, and other information concerning the need for, and consequences of, the intended regulation.

(8) Each agency shall identify and assess alternative forms of regulation and shall, to the extent feasible, specify performance objectives, rather than specifying the behavior or manner of compliance that regulated entities must adopt.

(9) Wherever feasible, agencies shall seek views of appropriate State, local, and tribal officials before imposing regulatory requirements that might significantly or uniquely affect those governmental entities. Each agency shall assess the effects of Federal regulations on State, local, and tribal governments, including specifically the availability of resources to carry out those mandates, and seek to minimize those burdens that uniquely or significantly affect such governmental entities, consistent with achieving regulatory objectives. In addition, as appropriate, agencies shall seek to harmonize Federal regulatory actions with related State, local, and tribal regulatory and other governmental functions.

(10) Each agency shall avoid regulations that are inconsistent, incompatible, or duplicative with its other regulations or those of other Federal agencies.

(11) Each agency shall tailor its regulations to impose the least burden on society, including individuals, businesses of differing sizes, and other entities (including small communities and governmental entities), consistent with obtaining the regulatory objectives, taking into account, among other things, and to the extent practicable, the costs of cumulative regulations.

(12) Each agency shall draft its regulations to be simple and easy to understand, with the goal of minimizing the potential for uncertainty and litigation arising from such uncertainty.

Sec. 2. *Organization.* An efficient regulatory planning and review process is vital to ensure that the Federal Government's regulatory system best serves the American people.

(a) *The Agencies.* Because Federal agencies are the repositories of significant substantive expertise and experience, they are responsible for developing regulations and assuring that the regulations are consistent with applicable law, the President's priorities, and the principles set forth in this Executive order.

(b) *The Office of Management and Budget.* Coordinated review of agency rulemaking is necessary to ensure that regulations are consistent with applicable law, the President's priorities, and the principles set forth in this Executive order, and that decisions made by one agency do not conflict with the policies or actions taken or planned by another agency. The Office of Management and Budget (OMB) shall carry out that review function. Within OMB, the Office of Information and Regulatory Affairs (OIRA) is the repository of expertise concerning regulatory issues, including methodologies and procedures that affect more than one agency, this Executive order, and the President's regulatory policies. To the extent permitted by law, OMB shall provide guidance to agencies and assist the President, the Vice President, and other regulatory policy advisors to the President in regulatory planning and shall be the entity that reviews individual regulations, as provided by this Executive order.

(c) *The Vice President.* The Vice President is the principal advisor to the President on, and shall coordinate the development and presentation of recommendations concerning, regulatory policy, planning, and review, as set forth in this Executive order. In fulfilling their responsibilities under this Executive order, the President and the Vice President shall be assisted by the regulatory policy advisors within the Executive Office of the President and by such agency officials and personnel as the President and the Vice President may, from time to time, consult.

Sec. 3. *Definitions.* For purposes of this Executive order: (a) "Advisors" refers to such regulatory policy advisors to the President as the President and Vice President may from time to time consult, including, among others: (1) the Director of OMB; (2) the Chair (or another member) of the Council of Economic Advisers; (3) the Assistant to the President for Economic Policy; (4) the Assistant to the President for Domestic Policy; (5) the Assistant to the President for National Security Affairs; (6) the Assistant to the President for Science and Technology; (7) the Assistant to the President for Intergovernmental Affairs; (8) the Assistant to the President and Staff Secretary; (9) the Assistant to the President and Chief of Staff to the Vice President; (10) the Assistant to the President and Counsel to the President; (11) the Deputy Assistant to the President and Director of the White House Office on Environmental Policy; and (12) the Administrator of OIRA, who also shall coordinate communications relating to this Executive order among the agencies, OMB, the other Advisors, and the Office of the Vice President.

(b) "Agency," unless otherwise indicated, means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(10).

(c) "Director" means the Director of OMB.

(d) "Regulation" or "rule" means an agency statement of general applicability and future effect, which the agency intends to have the force and effect of law, that is designed to implement, interpret, or prescribe law or policy or to describe the procedure or practice requirements of an agency. It does not, however, include:

(1) Regulations or rules issued in accordance with the formal rulemaking provisions of 5 U.S.C. 556, 557;

(2) Regulations or rules that pertain to a military or foreign affairs function of the United States, other than procurement regulations and regulations involving the import or export of non-defense articles and services;

(3) Regulations or rules that are limited to agency organization, management, or personnel matters; or

(4) Any other category of regulations exempted by the Administrator of OIRA.

(e) "Regulatory action" means any substantive action by an agency (normally published in the **Federal Register**) that promulgates or is expected

to lead to the promulgation of a final rule or regulation, including notices of inquiry, advance notices of proposed rulemaking, and notices of proposed rulemaking.

(f) "Significant regulatory action" means any regulatory action that is likely to result in a rule that may:

(1) Have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, or tribal governments or communities;

(2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another agency;

(3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs or the rights and obligations of recipients thereof; or

(4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in this Executive order.

Sec. 4. *Planning Mechanism.* In order to have an effective regulatory program, to provide for coordination of regulations, to maximize consultation and the resolution of potential conflicts at an early stage, to involve the public and its State, local, and tribal officials in regulatory planning, and to ensure that new or revised regulations promote the President's priorities and the principles set forth in this Executive order, these procedures shall be followed, to the extent permitted by law: (a) *Agencies' Policy Meeting.* Early in each year's planning cycle, the Vice President shall convene a meeting of the Advisors and the heads of agencies to seek a common understanding of priorities and to coordinate regulatory efforts to be accomplished in the upcoming year.

(b) *Unified Regulatory Agenda.* For purposes of this subsection, the term "agency" or "agencies" shall also include those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(10). Each agency shall prepare an agenda of all regulations under development or review, at a time and in a manner specified by the Administrator of OIRA. The description of each regulatory action shall contain, at a minimum, a regulation identifier number, a brief summary of the action, the legal authority for the action, any legal deadline for the action, and the name and telephone number of a knowledgeable agency official. Agencies may incorporate the information required under 5 U.S.C. 602 and 41 U.S.C. 402 into these agendas.

(c) *The Regulatory Plan.* For purposes of this subsection, the term "agency" or "agencies" shall also include those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(10). (1) As part of the Unified Regulatory Agenda, beginning in 1994, each agency shall prepare a Regulatory Plan (Plan) of the most important significant regulatory actions that the agency reasonably expects to issue in proposed or final form in that fiscal year or thereafter. The Plan shall be approved personally by the agency head and shall contain at a minimum:

(A) A statement of the agency's regulatory objectives and priorities and how they relate to the President's priorities;

(B) A summary of each planned significant regulatory action including, to the extent possible, alternatives to be considered and preliminary estimates of the anticipated costs and benefits;

(C) A summary of the legal basis for each such action, including whether any aspect of the action is required by statute or court order;

(D) A statement of the need for each such action and, if applicable, how the action will reduce risks to public health, safety, or the environment, as well as how the magnitude of the risk addressed by the action relates to other risks within the jurisdiction of the agency;

(E) The agency's schedule for action, including a statement of any applicable statutory or judicial deadlines; and

(F) The name, address, and telephone number of a person the public may contact for additional information about the planned regulatory action.

(2) Each agency shall forward its Plan to OIRA by June 1st of each year.

(3) Within 10 calendar days after OIRA has received an agency's Plan, OIRA shall circulate it to other affected agencies, the Advisors, and the Vice President.

(4) An agency head who believes that a planned regulatory action of another agency may conflict with its own policy or action taken or planned shall promptly notify, in writing, the Administrator of OIRA, who shall forward that communication to the issuing agency, the Advisors, and the Vice President.

(5) If the Administrator of OIRA believes that a planned regulatory action of an agency may be inconsistent with the President's priorities or the principles set forth in this Executive order or may be in conflict with any policy or action taken or planned by another agency, the Administrator of OIRA shall promptly notify, in writing, the affected agencies, the Advisors, and the Vice President.

(6) The Vice President, with the Advisors' assistance, may consult with the heads of agencies with respect to their Plans and, in appropriate instances, request further consideration or inter-agency coordination.

(7) The Plans developed by the issuing agency shall be published annually in the October publication of the Unified Regulatory Agenda. This publication shall be made available to the Congress; State, local, and tribal governments; and the public. Any views on any aspect of any agency Plan, including whether any planned regulatory action might conflict with any other planned or existing regulation, impose any unintended consequences on the public, or confer any unclaimed benefits on the public, should be directed to the issuing agency, with a copy to OIRA.

(d) *Regulatory Working Group.* Within 30 days of the date of this Executive order, the Administrator of OIRA shall convene a Regulatory Working Group ("Working Group"), which shall consist of representatives of the heads of each agency that the Administrator determines to have significant domestic regulatory responsibility, the Advisors, and the Vice President. The Administrator of OIRA shall chair the Working Group and shall periodically advise the Vice President on the activities of the Working Group. The Working Group shall serve as a forum to assist agencies in identifying and analyzing important regulatory issues (including, among others (1) the development of innovative regulatory techniques, (2) the methods, efficacy, and utility of comparative risk assessment in regulatory decision-making, and (3) the development of short forms and other streamlined regulatory approaches for small businesses and other entities). The Working Group shall meet at least quarterly and may meet as a whole or in subgroups of agencies with an interest in particular issues or subject areas. To inform its discussions, the Working Group may commission analytical studies and reports by OIRA, the Administrative Conference of the United States, or any other agency.

(e) *Conferences.* The Administrator of OIRA shall meet quarterly with representatives of State, local, and tribal governments to identify both existing and proposed regulations that may uniquely or significantly affect those governmental entities. The Administrator of OIRA shall also convene, from time to time, conferences with representatives of businesses, nongovernmental organizations, and the public to discuss regulatory issues of common concern.

Sec. 5. *Existing Regulations.* In order to reduce the regulatory burden on the American people, their families, their communities, their State, local, and tribal governments, and their industries; to determine whether regula-

tions promulgated by the executive branch of the Federal Government have become unjustified or unnecessary as a result of changed circumstances; to confirm that regulations are both compatible with each other and not duplicative or inappropriately burdensome in the aggregate; to ensure that all regulations are consistent with the President's priorities and the principles set forth in this Executive order, within applicable law; and to otherwise improve the effectiveness of existing regulations: (a) Within 90 days of the date of this Executive order, each agency shall submit to OIRA a program, consistent with its resources and regulatory priorities, under which the agency will periodically review its existing significant regulations to determine whether any such regulations should be modified or eliminated so as to make the agency's regulatory program more effective in achieving the regulatory objectives, less burdensome, or in greater alignment with the President's priorities and the principles set forth in this Executive order. Any significant regulations selected for review shall be included in the agency's annual Plan. The agency shall also identify any legislative mandates that require the agency to promulgate or continue to impose regulations that the agency believes are unnecessary or outdated by reason of changed circumstances.

(b) The Administrator of OIRA shall work with the Regulatory Working Group and other interested entities to pursue the objectives of this section. State, local, and tribal governments are specifically encouraged to assist in the identification of regulations that impose significant or unique burdens on those governmental entities and that appear to have outlived their justification or be otherwise inconsistent with the public interest.

(c) The Vice President, in consultation with the Advisors, may identify for review by the appropriate agency or agencies other existing regulations of an agency or groups of regulations of more than one agency that affect a particular group, industry, or sector of the economy, or may identify legislative mandates that may be appropriate for reconsideration by the Congress.

Sec. 6. ***Centralized Review of Regulations.*** The guidelines set forth below shall apply to all regulatory actions, for both new and existing regulations, by agencies other than those agencies specifically exempted by the Administrator of OIRA:

(a) ***Agency Responsibilities.*** (1) Each agency shall (consistent with its own rules, regulations, or procedures) provide the public with meaningful participation in the regulatory process. In particular, before issuing a notice of proposed rulemaking, each agency should, where appropriate, seek the involvement of those who are intended to benefit from and those expected to be burdened by any regulation (including, specifically, State, local, and tribal officials). In addition, each agency should afford the public a meaningful opportunity to comment on any proposed regulation, which in most cases should include a comment period of not less than 60 days. Each agency also is directed to explore and, where appropriate, use consensual mechanisms for developing regulations, including negotiated rulemaking.

(2) Within 60 days of the date of this Executive order, each agency head shall designate a Regulatory Policy Officer who shall report to the agency head. The Regulatory Policy Officer shall be involved at each stage of the regulatory process to foster the development of effective, innovative, and least burdensome regulations and to further the principles set forth in this Executive order.

(3) In addition to adhering to its own rules and procedures and to the requirements of the Administrative Procedure Act, the Regulatory Flexibility Act, the Paperwork Reduction Act, and other applicable law, each agency shall develop its regulatory actions in a timely fashion and adhere to the following procedures with respect to a regulatory action:

(A) Each agency shall provide OIRA, at such times and in the manner specified by the Administrator of OIRA, with a list of its planned regulatory actions, indicating those which the agency believes are significant regulatory

actions within the meaning of this Executive order. Absent a material change in the development of the planned regulatory action, those not designated as significant will not be subject to review under this section unless, within 10 working days of receipt of the list, the Administrator of OIRA notifies the agency that OIRA has determined that a planned regulation is a significant regulatory action within the meaning of this Executive order. The Administrator of OIRA may waive review of any planned regulatory action designated by the agency as significant, in which case the agency need not further comply with subsection (a)(3)(B) or subsection (a)(3)(C) of this section.

(B) For each matter identified as, or determined by the Administrator of OIRA to be, a significant regulatory action, the issuing agency shall provide to OIRA:

(i) The text of the draft regulatory action, together with a reasonably detailed description of the need for the regulatory action and an explanation of how the regulatory action will meet that need; and

(ii) An assessment of the potential costs and benefits of the regulatory action, including an explanation of the manner in which the regulatory action is consistent with a statutory mandate and, to the extent permitted by law, promotes the President's priorities and avoids undue interference with State, local, and tribal governments in the exercise of their governmental functions.

(C) For those matters identified as, or determined by the Administrator of OIRA to be, a significant regulatory action within the scope of section 3(f)(1), the agency shall also provide to OIRA the following additional information developed as part of the agency's decision-making process (unless prohibited by law):

(i) An assessment, including the underlying analysis, of benefits anticipated from the regulatory action (such as, but not limited to, the promotion of the efficient functioning of the economy and private markets, the enhancement of health and safety, the protection of the natural environment, and the elimination or reduction of discrimination or bias) together with, to the extent feasible, a quantification of those benefits;

(ii) An assessment, including the underlying analysis, of costs anticipated from the regulatory action (such as, but not limited to, the direct cost both to the government in administering the regulation and to businesses and others in complying with the regulation, and any adverse effects on the efficient functioning of the economy, private markets (including productivity, employment, and competitiveness), health, safety, and the natural environment), together with, to the extent feasible, a quantification of those costs; and

(iii) An assessment, including the underlying analysis, of costs and benefits of potentially effective and reasonably feasible alternatives to the planned regulation, identified by the agencies or the public (including improving the current regulation and reasonably viable nonregulatory actions), and an explanation why the planned regulatory action is preferable to the identified potential alternatives.

(D) In emergency situations or when an agency is obligated by law to act more quickly than normal review procedures allow, the agency shall notify OIRA as soon as possible and, to the extent practicable, comply with subsections (a)(3)(B) and (C) of this section. For those regulatory actions that are governed by a statutory or court-imposed deadline, the agency shall, to the extent practicable, schedule rulemaking proceedings so as to permit sufficient time for OIRA to conduct its review, as set forth below in subsection (b)(2) through (4) of this section.

(E) After the regulatory action has been published in the Federal Register or otherwise issued to the public, the agency shall:

(i) Make available to the public the information set forth in subsections (a)(3)(B) and (C);

(ii) Identify for the public, in a complete, clear, and simple manner, the substantive changes between the draft submitted to OIRA for review and the action subsequently announced; and

(iii) Identify for the public those changes in the regulatory action that were made at the suggestion or recommendation of OIRA.

(F) All information provided to the public by the agency shall be in plain, understandable language.

(b) *OIRA Responsibilities.* The Administrator of OIRA shall provide meaningful guidance and oversight so that each agency's regulatory actions are consistent with applicable law, the President's priorities, and the principles set forth in this Executive order and do not conflict with the policies or actions of another agency. OIRA shall, to the extent permitted by law, adhere to the following guidelines:

(1) OIRA may review only actions identified by the agency or by OIRA as significant regulatory actions under subsection (a)(3)(A) of this section.

(2) OIRA shall waive review or notify the agency in writing of the results of its review within the following time periods:

(A) For any notices of inquiry, advance notices of proposed rulemaking, or other preliminary regulatory actions prior to a Notice of Proposed Rulemaking, within 10 working days after the date of submission of the draft action to OIRA;

(B) For all other regulatory actions, within 90 calendar days after the date of submission of the information set forth in subsections (a)(3)(B) and (C) of this section, unless OIRA has previously reviewed this information and, since that review, there has been no material change in the facts and circumstances upon which the regulatory action is based, in which case, OIRA shall complete its review within 45 days; and

(C) The review process may be extended (1) once by no more than 30 calendar days upon the written approval of the Director and (2) at the request of the agency head.

(3) For each regulatory action that the Administrator of OIRA returns to an agency for further consideration of some or all of its provisions, the Administrator of OIRA shall provide the issuing agency a written explanation for such return, setting forth the pertinent provision of this Executive order on which OIRA is relying. If the agency head disagrees with some or all of the bases for the return, the agency head shall so inform the Administrator of OIRA in writing.

(4) Except as otherwise provided by law or required by a Court, in order to ensure greater openness, accessibility, and accountability in the regulatory review process, OIRA shall be governed by the following disclosure requirements:

(A) Only the Administrator of OIRA (or a particular designee) shall receive oral communications initiated by persons not employed by the executive branch of the Federal Government regarding the substance of a regulatory action under OIRA review;

(B) All substantive communications between OIRA personnel and persons not employed by the executive branch of the Federal Government regarding a regulatory action under review shall be governed by the following guidelines: (i) A representative from the issuing agency shall be invited to any meeting between OIRA personnel and such person(s);

(ii) OIRA shall forward to the issuing agency, within 10 working days of receipt of the communication(s), all written communications, regardless of format, between OIRA personnel and any person who is not employed by the executive branch of the Federal Government, and the dates and names of individuals involved in all substantive oral communications (including meetings to which an agency representative was invited, but did

not attend, and telephone conversations between OIRA personnel and any such persons); and

(iii) OIRA shall publicly disclose relevant information about such communication(s), as set forth below in subsection (b)(4)(C) of this section.

(C) OIRA shall maintain a publicly available log that shall contain, at a minimum, the following information pertinent to regulatory actions under review:

(i) The status of all regulatory actions, including if (and if so, when and by whom) Vice Presidential and Presidential consideration was requested;

(ii) A notation of all written communications forwarded to an issuing agency under subsection (b)(4)(B)(ii) of this section; and

(iii) The dates and names of individuals involved in all substantive oral communications, including meetings and telephone conversations, between OIRA personnel and any person not employed by the executive branch of the Federal Government, and the subject matter discussed during such communications.

(D) After the regulatory action has been published in the Federal Register or otherwise issued to the public, or after the agency has announced its decision not to publish or issue the regulatory action, OIRA shall make available to the public all documents exchanged between OIRA and the agency during the review by OIRA under this section.

(5) All information provided to the public by OIRA shall be in plain, understandable language.

Sec. 7. *Resolution of Conflicts.* To the extent permitted by law, disagreements or conflicts between or among agency heads or between OMB and any agency that cannot be resolved by the Administrator of OIRA shall be resolved by the President, or by the Vice President acting at the request of the President, with the relevant agency head (and, as appropriate, other interested government officials). Vice Presidential and Presidential consideration of such disagreements may be initiated only by the Director, by the head of the issuing agency, or by the head of an agency that has a significant interest in the regulatory action at issue. Such review will not be undertaken at the request of other persons, entities, or their agents.

Resolution of such conflicts shall be informed by recommendations developed by the Vice President, after consultation with the Advisors (and other executive branch officials or personnel whose responsibilities to the President include the subject matter at issue). The development of these recommendations shall be concluded within 60 days after review has been requested.

During the Vice Presidential and Presidential review period, communications with any person not employed by the Federal Government relating to the substance of the regulatory action under review and directed to the Advisors or their staffs or to the staff of the Vice President shall be in writing and shall be forwarded by the recipient to the affected agency(ies) for inclusion in the public docket(s). When the communication is not in writing, such Advisors or staff members shall inform the outside party that the matter is under review and that any comments should be submitted in writing.

At the end of this review process, the President, or the Vice President acting at the request of the President, shall notify the affected agency and the Administrator of OIRA of the President's decision with respect to the matter.

Sec. 8. *Publication.* Except to the extent required by law, an agency shall not publish in the Federal Register or otherwise issue to the public any regulatory action that is subject to review under section 6 of this Executive order until (1) the Administrator of OIRA notifies the agency that OIRA has waived its review of the action or has completed its review without

any requests for further consideration, or (2) the applicable time period in section 6(b)(2) expires without OIRA having notified the agency that it is returning the regulatory action for further consideration under section 6(b)(3), whichever occurs first. If the terms of the preceding sentence have not been satisfied and an agency wants to publish or otherwise issue a regulatory action, the head of that agency may request Presidential consideration through the Vice President, as provided under section 7 of this order. Upon receipt of this request, the Vice President shall notify OIRA and the Advisors. The guidelines and time period set forth in section 7 shall apply to the publication of regulatory actions for which Presidential consideration has been sought.

Sec. 9. *Agency Authority.* Nothing in this order shall be construed as displacing the agencies' authority or responsibilities, as authorized by law.

Sec. 10. *Judicial Review.* Nothing in this Executive order shall affect any otherwise available judicial review of agency action. This Executive order is intended only to improve the internal management of the Federal Government and does not create any right or benefit, substantive or procedural, enforceable at law or equity by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

Sec. 11. *Revocations.* Executive Orders Nos. 12291 and 12498; all amendments to those Executive orders; all guidelines issued under those orders; and any exemptions from those orders heretofore granted for any category of rule are revoked.

William J. Clinton

THE WHITE HOUSE,
September 30, 1993.

[FR Doc. 93-24523
Filed 10-1-93; 12:12 pm]
Billing code 3195-01-M

Editorial note: For the President's remarks on signing this Executive order, see issue 39 of the *Weekly Compilation of Presidential Documents.*

TAB
E

Contents

EVT/WOTE '10 Call for Papers

2010 Electronic Voting Technology Workshop/ Workshop on Trustworthy Elections (EVT/WOTE '10)

August 9–10, 2010
Washington, DC

Sponsored by USENIX: The Advanced Computing Systems Association; ACCURATE: A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections; and IAVoSS: The International Association for Voting System Sciences

EVT/WOTE '10 will be co-located with the 19th USENIX Security Symposium (USENIX Security '10), which will take place August 11–13, 2010.

Important Dates

- Submissions due: **April 16, 2010, 11:59 p.m. PDT**
- Notification of acceptance: **May 26, 2010**
- Final paper files due: **June 23, 2010**

Workshop Organizers
Program Co-Chairs
Doug Jones, *University of Iowa*
Jean-Jacques Quisquater, *Université catholique de Louvain*
Eric Rescorla, *RTFM, Inc.*

Program Committee
Josh Benaloh, *Microsoft Research*
Aaron Burstein, *University of California, Berkeley*
Michael Byrne, *Rice University*
Jeremy Epstein, *SRI*
Ari Feldman, *Princeton University*
Rop Gonggrijp
Alex Halderman, *University of Michigan, Ann Arbor*
Joseph Lorenzo Hall, *University of California, Berkeley, and Princeton University*
John Kelsey, *National Institute of Standards and Technology*
Sharon Laskowski, *National Institute of Standards and Technology*
Mark Lindeman, *Bard College*
Ron Rivest, *Massachusetts Institute of Technology*
Peter Ryan, *University of Luxembourg*
Olivier Pereira, *Université catholique de Louvain*
Hovav Shacham, *University of California, San Diego*
Vanessa Teague, *University of Melbourne*
Dan Wallach, *Rice University*

Overview
In many countries, most votes are counted and transported electronically, but there are numerous practical and policy implications of introducing electronic machines into the voting process. Both voting technology and its regulations are very much in flux, with open concerns including accuracy, reliability, robustness, security, transparency, equality, privacy, usability, and accessibility.

USENIX, ACCURATE, and IAVoSS are sponsoring the 2010 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE '10). EVT/WOTE brings together researchers from a variety of disciplines, ranging from computer science and human-computer interaction experts through political scientists, legal experts, election administrators, and voting equipment vendors. EVT/WOTE seeks to publish original research on important problems in all

aspects of electronic voting.

EVT/WOTE '10 will be a two-day event, Monday, August 9, and Tuesday, August 10, 2010, co-located with the 19th USENIX Security Symposium in Washington, DC. In addition to paper presentations, the workshop may include panel discussions with substantial time devoted to questions and answers. The workshop papers will be published electronically. Attendance at the workshop will be open to the public, although talks and refereed paper presentations will be by invitation only. There will be an award for the best paper.

Workshop Topics

Papers are solicited in all areas related to electronic voting, including but not limited to:

- Accessibility
- Analysis of/attacks on existing voting technologies
- Auditing
- Ballot integrity
- Ballot secrecy
- Case studies from the real world of elections
- Case studies of electronic voting experiments
- Design and implementation of new voting technologies
- Forensics
- Formal security analysis
- Impact of source code disclosure or nondisclosure
- Issues with and evolution of voting technology standards
- Legal issues including intellectual property
- Receipts and coercion resistance
- Risk assessement
- System testing methodologies
- Usability
- Verifiable election systems
- Vote collection/recording
- Vote tabulation
- Voter authentication
- Voter privacy and/or anonymity
- Voter registration and pre-voting processes
- Voting technology standards

Submission Instructions

Papers are due by Friday, April 16, 2010, at 11:59 p.m. PDT (firm deadline). All submissions will be made online via the Web form. Submissions should be finished, complete papers.

Paper submissions should be about 10 to a maximum of 16 typeset pages, formatted in one column, using 11 point Times Roman type on 12 point leading, in a text block of 6.5" by 9". Once accepted, papers must be reformatted to fit in 8 to 16 pages in a two-column format, using 10 point Times Roman type on 12 point leading, in a text block of 6.5" by 9". If you wish, please make use of this LaTeX style file and sample LaTeX file (see the corresponding PDF here) when preparing your paper for submission. The page limits are intended to include the bibliography and any appendices. Reviewers may not take into consideration any portion of a submission that is over the stated limit.

Paper submissions must be anonymized: both author names and author affiliations must be removed; acknowledgements and other clear markers of affiliation (e.g., "we used data from XXX University") should be removed or rewritten; self-citations should be rewritten to be neutral (e.g., "In previous work, Smith showed . . .").

Submissions must be in PDF format (i.e., processed by Adobe's Acrobat Distiller or equivalent). Note that LaTeX users can use the "dvipdf" command to convert a DVI file into PDF format. Please make sure your submission can be opened using Adobe Acrobat 4.0.

All submissions will be judged on originality, relevance, correctness, and clarity. Simultaneous submission of the same work to multiple venues, submission of previously published work, or plagiarism constitutes dishonesty or fraud. USENIX, like other scientific and technical

conferences and journals, prohibits these practices and may take action against authors who have committed them. See the USENIX Conference Submissions Policy for details. If authors have relevant submissions in other venues that are under review at the same time as their submission to the workshop, they should separately notify the program co-chairs. Questions? Contact your program co-chairs, evtwote10chairs@usenix.org, or the USENIX office, submissionspolicy@usenix.org.

Papers accompanied by nondisclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the USENIX EVT/WOTE '10 Web site; rejected submissions will be permanently treated as confidential.

Authors will be notified of acceptance by Wednesday, May 26, 2010. The final paper due date is Wednesday, June 23, 2010 (firm deadline). Each accepted submission may be assigned a member of the program committee to act as its shepherd through the preparation of the final paper. The assigned member will act as a conduit for feedback from the committee to the authors.

All papers will be available online to registered attendees before the workshop. If your accepted paper should not be published prior to the event, please notify production@usenix.org. The papers will be available online to everyone beginning on the first day of the workshop, August 9, 2010.

Specific questions about submissions may be sent to the program co-chairs at evtwote10chairs@usenix.org.

? Need help?
Last changed: 3 March 2010 ch

EVT/WOTE '10 Home
USENIX Home

Types of Priorities

When inviting applications for a competition using one or more priorities, we designate the type of each priority as absolute, competitive preference, or invitational through a notice the **Federal Register**. The effect of each type of priority follows:

Absolute priority: Under an absolute priority, we consider only applications that meet the priority (34 CFR 75.105(c)(3)).

Competitive preference priority: Under a competitive preference priority, we give competitive preference to an application by (1) awarding additional points, depending on the extent to which the application meets the priority (34 CFR 75.105(c)(2)(i)); or (2) selecting an application that meets the priority over an application of comparable merit that does not meet the priority (34 CFR 75.105(c)(2)(ii)).

Invitational priority: Under an invitational priority, we are particularly interested in applications that meet the priority. However, we do not give an application that meets the priority a preference over other applications (34 CFR 75.105(c)(1)).

Final Priority: We will announce the final priority in a notice in the **Federal Register**. We will determine the final priority after considering responses to this notice and other information available to the Department. This notice does not preclude us from proposing additional priorities, requirements, definitions, or selection criteria, subject to meeting applicable rulemaking requirements.

Note: This notice does *not* solicit applications. In any year in which we choose to use this priority, we invite applications through a notice in the **Federal Register.**

Executive Order 12866: This notice has been reviewed in accordance with Executive Order 12866. Under the terms of the order, we have assessed the potential costs and benefits of this proposed regulatory action.

The potential costs associated with this proposed regulatory action are those resulting from statutory requirements and those we have determined as necessary for administering this program effectively and efficiently.

In assessing the potential costs and benefits—both quantitative and qualitative—of this proposed regulatory action, we have determined that the benefits of the proposed priority justify the costs.

Discussion of Costs and Benefits

The benefits of the Disability and Rehabilitation Research Projects and Centers Programs have been well established over the years in that similar projects have been completed successfully. This proposed priority will generate new knowledge through research and development.

Another benefit of this proposed priority is that the establishment of a new RRTC will improve the lives of individuals with disabilities. The new RRTC will disseminate and promote the use of new information that will improve the options for individuals with disabilities to obtain, retain, and advance in employment.

Intergovernmental Review: This program is not subject to Executive Order 12372 and the regulations in 34 CFR part 79.

Accessible Format: Individuals with disabilities can obtain this document in an accessible format (*e.g.,* braille, large print, audiotape, or computer diskette) by contacting the Grants and Contracts Services Team, U.S. Department of Education, 400 Maryland Avenue, SW., room 5075, PCP, Washington, DC 20202–2550. Telephone: (202) 245–7363. If you use a TDD, call the FRS, toll free, at 1–800–877–8339.

Electronic Access to This Document: You can view this document, as well as all other documents of this Department published in the **Federal Register**, in text or Adobe Portable Document Format (PDF) on the Internet at the following site: *http://www.ed.gov/news/fedregister.* To use PDF you must have Adobe Acrobat Reader, which is available free at this site.

Note: The official version of this document is the document published in the **Federal Register**. Free Internet access to the official edition of the **Federal Register** and the Code of Federal Regulations is available on GPO Access at: *http://www.gpoaccess.gov/nara/index.html.*

Dated: April 20, 2010.

Alexa Posny,

Assistant Secretary for Special Education and Rehabilitative Services.

[FR Doc. 2010–9511 Filed 4–22–10; 8:45 am]

BILLING CODE 4000–01–P

ELECTION ASSISTANCE COMMISSION

Request for Substantive Comments on the EAC's Proposed Requirements for the Testing of Pilot Voting Systems To Serve UOCAVA Voters; Correction

AGENCY: United States Election Assistance Commission.

ACTION: Notice; correction.

SUMMARY: *This is a correcting to provide for a thirty day public comment period as reflected by commission tally vote.* The original notice incorrectly provided for a fifteen day public comment period. The U.S. Election Assistance Commission (EAC) is publishing for public comment a set of proposed requirements for the testing of pilot voting systems to be used by jurisdictions to serve Uniformed and Overseas voters.

FOR FURTHER INFORMATION CONTACT: Matthew Masterson, Phone (202) 566–3100, e-mail *votingsystemguidelines@eac.gov.*

Correction

In the **Federal Register** of March 31, 2010, on page 16090, in the first column, correct the **DATE** caption to read:

DATES: Comments must be received on or before 4 p.m. EST on April 30, 2010.

Alice Miller,

Chief Operating Officer, U.S. Election Assistance Commission.

[FR Doc. 2010–9384 Filed 4–22–10; 8:45 am]

BILLING CODE 6820–KF–P

DEPARTMENT OF ENERGY

Agency Information Collection Extension

AGENCY: U.S. Department of Energy.

ACTION: Notice and request for Comments.

SUMMARY: The Department of Energy (DOE), pursuant to the Paperwork Reduction Act of 1995, intends to extend, for three years, an information collection request with the Office of Management and Budget (OMB). Comments were invited on: (a) Whether the extended collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or other forms of information technology.

DATES: Comments regarding this proposed information collection must be received on or before June 22, 2010. If you anticipate difficulty in submitting comments within that period or if you want access to the collection of

U. S. Election Assistance Commission
Voting System Testing and Certification Program
1225 New York Avenue, NW, Suite 1100
Washington, DC. 20005

Recommendation for EAC Certification

To: Tom Wilkey, *Executive Director/Decision Authority*

From: Brian Hancock, Director, Testing and Certification Program

Date: April 2, 2010

RE: Waiver Request: Submission of Voting System Pilot Program Testing and Certification Manual For 15-day public comment period

---

Per the EAC's Notice and Public comment policy I am requesting a waiver from the 30-day public comment period under the policy and placing the document out for a 15-day public comment period. The reason for the shortened public comment period is to allow for the pilot certification program to be established in a timely manner in order to allow UOCAVA pilot systems to be submitted under the program in time to allow them to be used in the 2010 general election should a manufacturer desire to do so. In addition, because much of the manual is taken from already approved EAC manuals there is very little new material to review for comment.

Please indicate if the waiver is granted below:

✓ Waiver Granted

____ Waiver Denied

Thomas Wilkey
Executive Director, EAC

[FR Doc. 05–12685 Filed 6–28–05; 8:45 am]
BILLING CODE 6820–KF–C

ELECTION ASSISTANCE COMMISSION

Proposed Guidance on Voluntary Voting System Guidelines

AGENCY: United States Election Assistance Commission (EAC).

ACTION: Notice of proposed voluntary Voting System Guidelines and request for comments.

SUMMARY: EAC is proposing Voluntary Voting System Guidelines pursuant to sections 221 and 222 of the Help America Vote Act of 2002 (HAVA) which was passed by Congress to modernize the administration of Federal elections. This marks the first time in our nation's history that the Federal Government has funded an election reform effort. HAVA provides Federal funding to help the States meet the law's uniform and non-discretionary administrative requirements, which include the following new programs and procedures: (1) Provisional voting, (2) voting information, (3) statewide voter registration lists and identification requirements for first-time registrants, (4) administrative complaint procedures, and (5) updated and upgraded voting equipment.

HAVA also established the U.S. Election Assistance Commission (EAC) to administer the Federal funding and to provide guidance to the States in their efforts to comply with the HAVA administrative requirements. Section 202 directs the EAC to adopt voluntary voting system guidelines, and to provide for the testing, certification, decertification, and recertification of voting system hardware and software. The purpose of the guidelines is to provide a set of specifications and requirements against which voting systems can be tested to determine if they provide all the basic functionality, accessibility, and security capabilities required of voting systems.

This document, the Voluntary Voting System Guidelines, is the third iteration of national level voting system standards. The Federal Election Commission published the Performance and Test Standards for Punchcard, Marksense and Direct Recording Electronic Voting Systems in 1990. This was followed by the Voting Systems Standards in 2002.

As required by HAVA, EAC formed the Technical Guidelines Development Committee (TGDC) to develop an initial set of recommendations for the Guidelines. This committee of 15 experts began their work in July 2004 and submitted their recommendations to the EAC in the 9-month timeline prescribed by HAVA. The TGDC was provided with technical support by the National Institute for Standards and Technology (NIST), who was given nearly $3 million dollars by the EAC to complete this work. This funding represents the first time the Federal Government has spent a significant amount of money on setting guidelines for voting systems. These latest Guidelines update and augment the 2002 Voting Systems Standards to address increasingly complex voting system technology. Specifically, the 2005 Guidelines address the critical topics of accessibility, usability, and security. These Guidelines are voluntary. States may adopt them in whole, in part, or not at all. States may also choose to enact stricter performance requirements for certifying their voting systems.

The Guidelines consist of two volumes. Volume I, entitled ''Voting System Performance Guidelines,'' includes new requirements for accessibility, voting system software distribution, system setup validation, and the use of wireless communications. This volume also includes a set of optional requirements for a Voter Verified Paper Audit Trail component for Direct Recording Electronic voting systems for use by those States that have decided to require this feature for their voting systems. In addition, it contains an updated glossary and a conformance clause. Volume II, entitled ''Voting System National Certification Guidelines,'' has been revised to reflect the new EAC process for national certification of voting systems. This process will go into effect in 2005 and will replace the voting system qualification process that has been conducted by the National Association of State Election Directors since 1994. Volume II also includes an updated appendix on procedures for testing system error rates. Terminology in both volumes has been revised to reflect new terminology introduced by HAVA. The following provides a summary of the contents of each volume.

Volume I Summary: Volume I, the Voting System Performance Guidelines, describes the requirements for the electronic components of voting systems. It is intended for use by the broadest audience, including voting system developers, manufacturers and suppliers; voting system testing labs; state organizations that certify systems prior to procurement; state and local election officials who procure and deploy voting systems; and public interest organizations that have an interest in voting systems and voting system standards. It contains the following sections:

- Section 1 presents the objectives and usage of the Guidelines, definitions of types of voting systems, and a discussion of how the guidelines and testing specifications are applied. It also contains a conformance clause.
- Section 2 describes the functional capabilities required of voting systems.
- Sections 3 through 5 describe specific performance standards for election system hardware, software and telecommunications.
- Section 6 is a significantly expanded section on security requirements for voting systems. It includes new material for the secure distribution of voting system software and for verifying that voting systems are operating with the correct software. There are also new requirements for the use of wireless communications. Since some States have decided to require a voter verified paper audit trail component for their direct recording electronic (DRE) voting systems, requirements are included to support appropriate testing of these components. These requirements are optional because there are other currently available technologies besides paper audit trails that can be employed to provide a second method, in addition to the DRE summary screen, for voters to verify their ballot choices. There was insufficient time to develop requirements for these other technologies for the present Guidelines, but these technologies, including audio, video, and cryptographic means, will be addressed in the near future.
- Sections 7 and 8 describe requirements for vendor quality assurance and configuration management practices and the documentation required about these practices for the certification process.
- Appendix A contains a glossary of terms.
- Appendix B provides a list of documents incorporated into the Guidelines by reference, as well as documents used in preparation of the Guidelines.
- Appendix C contains best practices for election officials regarding accessibility, paper audit trails, and wireless.
- Appendix D presents an informational discussion of independent dual verification which is a concept being examined for potential future application to voting systems. In essence, this is a methodology to produce multiple independent records

of ballot choices for verification purposes. Voter verified paper audit trails do not provide independent verification because the printer prints from the same data source that produces the DRE summary screen display.

• Appendix E contains the NASED Voting System Standards Board Technical Guide #1 on color and contrast adjustment for individuals with low vision or color blindness.

Volume II Summary: Volume II, the Voting System National Certification Testing Guidelines, is a complementary document to Volume I. Volume II provides an overview and specific detail of the national certification testing process, which is performed by independent voting system test labs accredited by the EAC. It is intended principally for use by vendors, test labs, and election officials who certify, procure, and accept voting systems. This volume contains the following sections:

• Section 1 presents an overview of the testing guidelines and the national certification testing process.

• Section 2 provides a description of the Technical Data Package that vendors are required to submit with their system for certification testing.

• Section 3 describes the basic functionality testing requirements.

• Sections 4 through 6 define the requirements for hardware, software and system integration testing.

• Section 7 describes the required examination of vendor quality assurance and configuration management practices.

• Appendix A provides the requirements for the National Certification Test Plan that is prepared by the voting system test lab and provided to the EAC for review.

• Appendix B describes the scope and content of the National Certification Test Report which is prepared by the test lab and delivered to the EAC along with a recommendation for certification.

• Appendix C describes the guiding principles used to design the voting system certification testing process. It also contains a revised section on testing system error rates.

The format of the Guidelines is intended to facilitate ease of identifying new information and comparison with the 2002 Voting Systems Standards. New material is indicated by a gray-shaded header with the words ''NEW MATERIAL,'' and includes line numbers. Material essentially carried forward in its entirety from the 2002 Voting Systems Standards remains in its original format and does not include line numbers. Selected portions of this material have been revised to reflect the EAC process for voting system certification, specifically Volume I, Section 1.6.1, and Volume II Section 1. Updates have been made throughout to include new terminology introduced by HAVA.

Comments: The Voluntary Voting System Guidelines is provided for comment by the public for the next 90 days. All comments must be received by EAC on or before 5 p.m. EDT on September 30, 2005. All comments will posted on the EAC Web site. The EAC is provided several alternative methods for submitting comments.

• On-line electronic comment form at *http://www.eac.gov.*

• By e-mail to *votingsystemguidelines@eac.gov.*

• By mail to Voting System Guidelines Comments, U.S. Election Assistance Commission, 1225 New York Ave, NW., Suite 1100, Washington, DC 20005.

• By fax to Voting System Guidelines Comments at (202) 566–3127.

EAC requests that comments be provided according to the following specifications:

(1) Comments regarding a particular section should be designed by the page, line (if included) and section number to which the comment refers.

(2) Comments regarding a term that is included or that should be added to the glossary should reference the term and page number to which the comment refers.

(3) General comments regarding the entire document or comments that refer to more than one section should be made as specifically as possible so that EAC can clearly understand to which portion(s) of the documents the comment refers.

(4) To the extent that a comment suggests a change in the wording of a requirement or section of the Guidelines, please provide proposed language for the suggested change.

To obtain a copy of the voluntary voting system guidelines: Due to the fact that the Voluntary Voting System Guidelines is more than 250 pages in length, the entire documents has not been attached to this notice. A complete copy of the Voluntary Voting System Guidelines is available from EAC in electronic or hard copy format. An electronic copy can be downloaded in PDF format or read in HTML version on EAC's Web site, *http://www.eac.gov*. In addition, interested persons may obtain a hard copy or CD–ROM electronic copy from EAC by contacting Voting System Guidelines, via fax at 202–566–3128, via e-mail at *VotingSystemGuidelines@eac.gov*, or via mail at Voting System Guidelines, U.S. Election Assistance Commission, 1225 New York Avenue, NW., Suite 1100, Washington, DC 20005. You may also request by phone at (866) 747–1471. Please specify whether a hard copy or electronic copy is desired.

FOR FURTHER INFORMATION CONTACT: Carol A. Paquette, Phone (202) 566–3125, fax (202) 566–3128, e-mail *cpaquette@eac.gov*.

Thomas R. Wilkey,

Executive Director, U.S. Election Assistance Commission.

[FR Doc. 05–12859 Filed 6–28–05; 8:45 am]

BILLING CODE 6820–KF–M

DEPARTMENT OF ENERGY

Office of Energy Efficiency and Renewable Energy

Federal Energy Management Advisory Committee

AGENCY: Department of Energy.

ACTION: Notice of open meeting.

SUMMARY: This notice announces an open meeting of the Federal Energy Management Advisory Committee (FEMAC). The Federal Advisory Committee Act (Public Law 92–463, 86 Stat. 770) requires that these meetings be announced in the **Federal Register** to allow for public participation. This notice announces the tenth FEMAC public meeting, an advisory committee established under Executive Order 13123—''Greening the Government through Efficient Energy Management.''

DATES: Monday, August 15, 2005; 6 to 7 p.m.

ADDRESSES: Long Beach Convention Center, 300 East Ocean Boulevard, Room 101, Long Beach, CA 90802.

FOR FURTHER INFORMATION CONTACT: Rick Klimkos, Designated Federal Officer, Office of Federal Energy Management Programs, U.S. Department of Energy, 1000 Independence Avenue, SW., Washington, DC 20585; (202) 586–8287.

SUPPLEMENTARY INFORMATION:

Purpose of the Meeting: To seek input and feedback from interested parties on working group recommendations to meet mandated Federal energy management goals.

Tentative Agenda: Agenda will include discussions on the following topics:

○ Update on FEMAC Working Groups.

○ Discussion on FEMAC priorities.

○ Open discussion with public.

Public Participation: In keeping with procedures, members of the public are welcome to observe the business of the

United States
Election Assistance Commission
1225 New York Avenue N.W. - Suite 1100
Washington, DC 20005

For Immediate Release

10/31/2007

Contact:
Bryan Whitener, Jeannie Layson
(202) 566-3100

EAC Seeks Public Comment on TGDC's Recommended Voluntary Voting System Guidelines -- Online Comment Tool Now Available

WASHINGTON – The United States Election Assistance Commission (EAC) has launched the first of two public comment periods on the draft voluntary voting system guidelines (VVSG) prepared by EAC's Technical Guidelines Development Committee (TGDC). The public is now able to submit comments about the draft guidelines by accessing the comment tool available at www.eac.gov. The public will also be able to view the comments submitted. Comments will be accepted through the online comment tool or by mailing them to EAC at 1225 New York Avenue NW, Suite 1100, Washington DC, 20005.

"The initial public comment phase is only the first step in EAC's inclusive and thorough approach as we move toward the adoption of the next iteration of voluntary voting system guidelines," said EAC Chair Donetta Davidson. "Throughout the process, public input and involvement will be extremely important to the EAC, and we will review each and every comment that is submitted. We strongly encourage everyone to participate in this important review process."

The draft guidelines were prepared by the TGDC and delivered to EAC in August and posted on the EAC's Web site. The introduction of the public comment tool launches the first of four phases leading to the adoption of a final version.

Phase I – The EAC submits the TGDC's draft document to the Federal Register and launches the **first public comment phase** with an online comment tool available at www.eac.gov. The public comment period will last for 120 days and all comments will be made public. Also during this phase the EAC will hold public meetings with stakeholders to discuss the proposed guidelines.

Phase II – The EAC will collect and review all public comments submitted on the TGDC draft. After consideration of all public comments, the EAC will perform an internal review.

Phase III – Based upon public comment and internal review of the TGDC document, the EAC will develop and publish its draft version in the Federal Register. **The public will have another 120 days to comment on the EAC draft version**. The EAC will conduct public hearings about its draft version.

Phase IV – The EAC will collect and review all comments submitted and make final modifications. The final version of the VVSG will be adopted by vote of the Commission at a public meeting and then published in the Federal Register.

One of EAC's most important mandates under the Help America Vote Act (HAVA) is the testing, certification, decertification, and recertification of voting system hardware and software. The VVSG provide a set of specifications and requirements against which voting systems can be tested to determine if they provide all the basic functionality, accessibility, and security capabilities required of voting systems. According to HAVA, adoption of the VVSG at the state level is voluntary. However, states may formally adopt the VVSG, making these guidelines mandatory in their jurisdictions.

The draft guidelines, which were prepared by the TGDC, are a complete re-write of the 2005 guidelines, intended to address the next generation of voting systems. These guidelines contain new and expanded material in the areas of reliability and quality, usability and accessibility, security, and testing. The draft guidelines require software independence, a concept created for purposes of the TGDC draft as a high level security requirement for all voting systems. According to the TGDC draft guidelines, software independence can be achieved through the use of independent voter verifiable records (IVVR) or through the innovation class. Additionally, the TGDC draft recommends open-ended vulnerability testing (OEVT), a testing method designed to bring greater security to voting systems in the polling place.

History of Voting System Standards and Guidelines

The first set of national voting system standards was created in 1990 by the Federal Election Commission (FEC). In 2002, the FEC updated the standards (2002 VSS). With the passage of the Help America Vote Act of 2002 (HAVA), EAC was assigned the responsibility of updating these standards, which would be known as the Voluntary Voting System Guidelines. HAVA also instructed the EAC, along with its Federal advisory committee, the Technical Guidelines Development Committee (TGDC), and the National Institute of Standards and Technology (NIST), to work collaboratively to develop the VVSG.

On December 13, 2005, the EAC adopted the VVSG. Before the adoption of the VVSG, the EAC conducted a thorough and transparent public comment process. After conducting an initial review of the draft VVSG, the EAC released the two-volume proposed guidelines for 90-day public comment period; during this period, the EAC received more than 6,000 comments. Each comment was reviewed and considered before the document was finalized and adopted, and all comments were posted on the EAC Web site. The EAC held public hearings about the VVSG in New York City, NY; Pasadena, CA; and Denver, CO. The final version was adopted at the public meeting in December 13, 2005.

EAC is an independent bipartisan commission created by the HAVA. EAC serves as a national clearinghouse and resource of information regarding election administration. It is charged with administering payments to states and developing guidance to meet HAVA requirements, adopting voluntary voting system guidelines, and accrediting voting system test laboratories and certifying voting equipment. It is also charged with developing and maintaining a national mail voter registration form. The four EAC commissioners are Donetta Davidson, chair; Rosemary Rodriguez, vice chair; Caroline Hunter; and Gracia Hillman.

# # #

Appendix IV: Comments from the Election Assistance Commission

U. S. ELECTION ASSISTANCE COMMISSION
OFFICE OF THE EXECUTIVE DIRECTOR
1225 New York Avenue, NW, Suite 1100
Washington, DC. 20005

May 25, 2007

Mr. Derek B. Stewart
Director, Defense Capabilities
And Management
Government Accountability Office
Washington, DC 20548

RE: Comments regarding proposed GAO-07-774 Report:

Mr. Stewart:

Thank you for the opportunity to comment on the GAO report entitled: *ELECTIONS: Action Plans Needed to Fully Address Challenges in Electronic Absentee Voting Initiatives for Military and Overseas Citizens (GAO-07-774)* submitted to the Election Assistance Commission (EAC) on May 10, 2007. The EAC appreciates GAO's accuracy in its portrayal of the EAC and its current activities regarding military and overseas voters. The EAC is grateful to GAO for its recognition of the EAC's current research efforts to engage election officials and UOCAVA voters prior to the development of these guidelines for military and overseas voters. The EAC also accepts the recommendations as outlined in the report and has begun efforts to achieve the goals as provided to us in the recommendation.

As noted in your report, for the EAC's 2007 research on military and overseas voters, the EAC is conducting the largest survey of UOCAVA voters ever conducted. This survey of ten thousand UOCAVA voters is designed to explore the challenges faced by those voters and determine what solutions have been effective in meeting their unique needs as overseas voters. At last update the EAC had received five thousand replies to the survey and is anticipating more before the data is compiled. As surveys go, this is an excellent response at this point in the process. Based on the replies already received, the EAC is extremely optimistic that the survey results will provide an invaluable look into the UOCAVA experience, and guidance leading to the development of guidelines that are realistic and effective. Also as part of this study, the EAC is conducting case studies of four states that are using new techniques in technology to meet the needs of their UOCAVA voters. The EAC has scheduled a conference to discuss the research results in September of 2007. The EAC will invite election officials, FVAP, NIST, the Overseas Vote Foundation, and other stakeholders to discuss the results of the research and possible solutions to the problems UOCAVA voters face. Also at the conference, the EAC will be conferring with officials from the four states that are participating in the EAC's case studies in order to further explore the unique ways that these states are meeting the demands of their military and overseas voters, and thus help shape the agenda for future guidelines development.

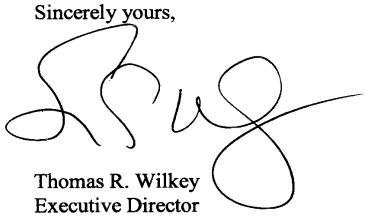
In response to one of the recommendations presented in the report, the EAC would like to note its constant and continued use of election officials in its projects. Besides the election officials who are appointed to the three statutory boards who are regularly updated on EAC projects, the EAC constantly updates election officials throughout the country on research and ongoing projects in order to ensure the work is accurate and useful. The EAC recognizes how important input from these officials is and will continue to work with them, especially those who use creative or new solutions to serve UOCAVA voters.

The EAC would like to reiterate its long held belief that National Institute of Standards and Technology (NIST), because of its internationally recognized technical expertise in developing standards, is essential to the development of voting guidelines for UOCAVA voters. NIST has in the past played a critical role in the development of voting system guidelines. With NIST's guidance the EAC released the newest version of the Voluntary Voting System Guidelines (VVSG) in 2005. Currently NIST is working with the EAC's Technical Guidelines Development Committee to create the next iteration of the VVSG which is a total re-write of VVSG 2005. NIST has consulted FVAP on a several occasions in the past to assist them in regard to UOCAVA voting and the use of the internet.

The EAC has met with FVAP and NIST and reached an agreement to work over the next several months to develop a timeline for the creation of UOCAVA guidelines. We all agree that the release of the EAC's UOCAVA study in September 2007 will be an important first step in this process as it will provide valuable information to help inform the guideline development process. Prior to the release of our study, the EAC, FVAP, and NIST will continue to meet in order to create a reasonable timeline for the creation of the guidelines pursuant to your recommendations.

Again, the EAC would like to thank GAO for the careful analysis of our work in this report and the recommendations to us. The Commission views this issue very seriously and GAO's guidance on this matter is greatly appreciated. We look forward to continued work with FVAP and NIST on this matter and eventually the successful creation of realistic and effective UOCAVA absentee ballot guidelines. Should you have any further questions, please feel free to contact me at (202) 566-3109 or twilkey@eac.gov.

Sincerely yours,



Thomas R. Wilkey
Executive Director

THE NATIONAL ACADEMIES
Advisers to the Nation on Science, Engineering, and Medicine

Computer Science and Telecommunications Board

500 Fifth Street, NW
Washington, DC 20001
Phone: 202 334 2605
Fax: 202 334 2318
E-mail: cstb@nas.edu
www.cstb.org

July 20, 2006

Lawrence Brandt
Program Director
Information Integration & Informatics (III) Cluster
Directorate for Computer and Information Sciences and Engineering
National Science Foundation
4201 Wilson Boulevard
Arlington, Virginia 22230

Dear Dr. Brandt:

With this letter report,[1] the National Research Council's Committee on a Framework for Understanding Electronic Voting (Appendix A) seeks to provide some idea of the current state of readiness for electronic voting in jurisdictions across the United States and to gauge what progress has been made since the publication of the committee's 2005 report, *Asking the Right Questions About Electronic Voting*.[2] This second report of the committee is based on a May 2006 workshop that brought together a number of knowledgeable and thoughtful local, state, and federal election officials (Appendix B) who shared their perspectives and experiences with the committee.[3] Presentations and discussions at the workshop made clear that many of the issues

---

[1] The preparation of this letter report was supported under National Science Foundation Award Number IIS-0436133. However, in accordance with National Research Council policy, the NSF did not review this report before publication, and the opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the NSF.

[2] For more information, see National Research Council, *Asking the Right Questions About Electronic Voting*, The National Academies Press, Washington, D.C., 2005. See also http://www.cstb.org/pub_evoting.html.

[3] The analysis, conclusions, and recommendations presented in this letter report are the responsibility of the committee alone and should not be attributed to these officials or anyone else. Furthermore, the justification for the committee's conclusions and recommendations does not lie in a statistically valid sampling of the nation's voting jurisdictions but is instead based on a mix of inputs. Testimony to the committee by the officials listed in Appendix B was intended to put a human and contemporary face on the nature of difficulties that jurisdictions are likely to face if problems arise in conducting the November 2006 elections.

discussed in *Asking the Right Questions* remain open and quite fluid as the nation approaches the 2006 elections—these issues include reliability, usability, security, training, education, and testing/certification.

The scope of this letter report is restricted to readiness for using electronic voting systems, by which is meant the systems with which voters interact directly to cast their ballots. Direct recording electronic (DRE) systems are the most obvious example, but electronic voting systems also include optical scan systems. In these latter systems, the voter marks his or her preferences on a physical paper ballot; the ballot is then read by an optical scanner, and the vote is passed to a tabulation mechanism for counting. This report is concerned primarily with readiness for the November 2006 elections, rather than with longer-term issues. For a discussion of longer-term issues, the reader is advised to consult *Asking the Right Questions*.

CURRENT STATUS OF PREPARATION FOR THE NOVEMBER 2006 ELECTIONS

On the basis of the testimony of the local, state, and federal election officials present at the workshop, the expertise developed by the committee in preparing its September 2005 report, and the experience and background of individual committee members, the committee believes that some jurisdictions—and possibly many—may not be well prepared for the arrival of the November 2006 elections with respect to the deployment and use of electronic voting equipment and related technology, and anxiety about this state of affairs among election officials is evident in a number of jurisdictions. Several factors appear to contribute to this unease and concern:

- *Compliance deadlines tied to the November 2006 elections that are required by the Help America Vote Act (HAVA)*. Some states and jurisdictions have failed to meet HAVA-mandated deadlines already, and others are likely to miss deadlines tied to the November 2006 election (and thus will carry out the fall elections with equipment and systems that are not HAVA-compliant), although it remains to be seen what legal or political consequences, if any, will flow from these missed deadlines. Other jurisdictions will meet HAVA deadlines in a technical sense but may not be able to fulfill certain key HAVA objectives, such as increasing voting booth accessibility for disabled voters or reducing the error rate in the ballots cast.[4] In still other cases, jurisdictions rushing to meet deadlines for HAVA compliance might have done so in counterproductive ways, such as by buying equipment that is not up to par, using software that may not be fully compatible with existing applications, not becoming sufficiently familiar with vendor products, and so on.
- *State legislative activity*. Entirely apart from HAVA, many states have imposed additional requirements for election equipment and have set new requirements for election procedures. For example, at least 26 states have passed laws mandating that voter-verified paper audit trails (VVPATs) be provided for voting

[4] Issues related to reducing voter error rates are discussed in *Asking the Right Questions*, pp. 82-95.

equipment that will be used in the November elections.[5] For some of the states that are using retrofitted DRE systems, the 2006 primary election represents the first large-scale use of VVPAT-equipped voting systems.[6] That is, the concept of voter verification of votes cast on DRE systems has never been tested on a large scale in any U.S. election, and the impact of this particular capability on election results and public confidence in them has yet to be seen.

- *Security*. Security issues remain prominent in the public debate about voting technologies.[7] For example, even as the committee was meeting, concerns were spreading about a new vulnerability discovered in one prominent vendor's equipment.[8] On June 27, 2006, New York University's Brennan Center for Justice released a report focusing on security vulnerabilities in electronic voting machines.[9] Physical security was also discussed at the workshop—with one official recounting the difficulties in providing adequate warehousing space for her e-voting equipment, as well as concerns about how to transport such equipment safely and securely.
- *Vendor performance*. Several workshop participants in contractual relationships with two prominent vendors reported on nontrivial problems with poorly designed, poorly tested, or poorly constructed e-voting equipment. For example, equipment has been delivered with many sample defects, including such things as sharp edges on machines and broken legs on machine stands. In other cases, some vendors are meeting promises regarding delivery of equipment by supplying for shared use equipment that has been used in other jurisdictions. Such sharing has been possible when (primary) elections are held on different dates, but this tactic obviously cannot be used on November 7, 2006.
- *Poll worker availability*.[10] In some jurisdictions, the availability of trained poll workers may be an issue in the fall. Some election officials at the workshop

---

[5] See, for example, http://www.verifiedvoting.org.

[6] A modern DRE system usually has a screen that displays the ballot to voters. For accepting input, some have touch screens, while others use mechanical selection devices. When the voter is finished voting, the voter takes some action in front of the machine to finalize his or her ballot. When a VVPAT is attached to the system, the voter has the opportunity to view a paper record of his or her vote that is then stored with the system just before the finalization action is taken. See *Asking the Right Questions*, pp. 39-42.

[7] For more discussion of security issues, see *Asking the Right Questions*, pp. 57-82.

[8] See Monica Davey, "New Fears of Security Risks in Electronic Voting Systems," *New York Times*, May 12, 2006. Available at http://www.nytimes.com/2006/05/12/us/12vote.html?ex=1305086400&en=5b3554a76aad524a&ei=5090&partner=rssuserland&emc=rss.

[9] Brennan Center Task Force on Voting System Security, *The Machinery of Democracy: Protecting Elections in an Electronic World*, Brennan Center, New York University, New York, 2006. Available at http://www.brennancenter.org/programs/downloads/Full%20Report.pdf.

[10] See *Asking the Right Questions*, pp. 100-105.

reported concerns that they will not be able to train enough poll workers in how to use the new equipment for November, a prospect that they believe will result in very long lines, excessive delays, and voter confusion if poll workers are unable to answer questions about the new systems. Poll workers must be trained in system setup and basic troubleshooting, as well as in answering questions that voters are likely to have—and even poll workers with experience from past elections may not be of much assistance to voters if they themselves are unfamiliar with the electronic voting systems at their polling places.

- *Voter education*.[11] For many voters, the November 2006 election will be the first conducted with electronic voting systems. Election officials are concerned about voter readiness to use these new technologies, as well as the related question of citizen confidence in the newly deployed systems.

This set of observations is not intended to suggest that all jurisdictions are facing these issues with the same concern and intensity. Indeed, perhaps the committee's most salient impression as the nation approaches the fall elections is the wide variation in the situations of the various jurisdictions, the consequences and implications of which remain to be seen.

EMERGING FACTORS AND REALIZATIONS

As jurisdictions proceed along the path toward electronic voting in November 2006, a number of factors are becoming more apparent.

First, jurisdictions are becoming more aware of the cost implications of deploying electronic voting systems, in particular, the fact that the initial acquisition cost of an electronic voting system is only a fraction of the total life-cycle cost.[12] Furthermore, HAVA appropriations represent a one-time infusion of federal money to the states (most of which has already been spent on equipment purchases),[13] and no supplemental funds are likely to be forthcoming from either the federal government or the states for conducting elections. Thus, many jurisdictions are facing the November elections without adequate financial resources to address the problems they see on the horizon—problems including equipment testing; maintenance and storage; training of poll workers; and voter education.

A second factor is that as some jurisdictions have learned for themselves about the complexities of electronic voting, their relationships with e-voting equipment vendors and service providers have become increasingly adversarial. For example, a number of workshop participants reported that they have become more assertive in their dealings with vendors and are less willing to accept what they believe to be shoddy work or broken promises: some reported having developed more leverage and expertise in negotiating contracts and terms with vendors. But other workshop participants reported having problems with and less success in obtaining desirable provisions for contracts

[11] See *Asking the Right Questions*, pp. 93-95.
[12] See *Asking the Right Questions*, p. 97.
[13] See *Asking the Right Questions*, p. 114.

they were negotiating. Also, some workshop participants reported that colleagues from smaller jurisdictions with fewer resources, and perhaps lacking the necessary legal, technical, or contracting expertise to negotiate more favorable terms, simply accept the standard vendor contract.[14]

Third, election officials are increasingly realizing the fundamental contradictions between relying on current procedures and requirements for certifying voting system software,[15] on the one hand, and holding elections on fixed, immovable dates, on the other.[16] The fundamental reality of software is that problems can emerge after the software has been certified and put into use, and some of these problems may be serious enough to require fixing. However, ensuring that the installation of a fix does not have other, unintended consequences (e.g., causing yet another problem) can be a difficult process, and re-certification of modified software can be quite time-consuming. Yet elections are held on the first Tuesday of November and are postponed only under extraordinary and rare circumstances—and it is unlikely that the lack of certification for a patched software system would be regarded by election officials as such an extraordinary circumstance. Thus, in the event that problems are found after certification, election officials must then choose between using certified systems with known problems or using uncertified systems in which those problems may have been fixed—and the latter may be regarded by some election officials as the lesser of two evils.

A fourth factor is the extent and scope of vendor involvement apart from the sale of equipment itself.[17] For example:

- Workshop participants expressed considerable skepticism about current certification processes for electronic voting systems,[18] given the lack of an arms-length relationship between the independent testing authorities (ITAs) and the vendors. Rightly or wrongly, these concerns originate in the fact that vendors pay the ITAs for undertaking certification.[19] In addition, vendors have opportunities to tune their software specifically for the tests in question, a practice somewhat akin to studying for a test rather than learning the material in a course. Lack of certification reform has also contributed to such skepticism.

---

[14] The group of election officials assembled for this workshop agreed that their jurisdictions have relatively greater access to resources than do most other jurisdictions and thus are not necessarily representative of most jurisdictions across the nation. The committee also noted that most voting jurisdictions in the nation are on the smaller side.

[15] Note that software is used in electronic ballot marking systems and electronic tabulation systems, and both generally require certification.

[16] See *Asking the Right Questions*, pp. 110-114.

[17] See *Asking the Right Questions*, pp. 120-122.

[18] See *Asking the Right Questions*, pp. 110-114.

[19] The mere fact that a vendor pays for a testing procedure should not itself be damning. For example, Underwriters Laboratory has provided product certification for many years. Although product manufacturers pay for the testing and certification process, UL certification has some notable credibility in the marketplace.

- In some cases (involving both DRE and optical scan systems), vendors are responsible for generating the various vote counts that emerge from an election—a function that has traditionally and historically been an inherently governmental function. Although election officials continue to have ultimate responsibility for the integrity of an election even when privatized vote counting is in place, vendors with profit-making motives have high incentives to cut corners and to refrain from incurring costs in resolving disputed votes.
- Electronic voting equipment is complex and thus requires considerably more training to operate (especially with respect to troubleshooting issues). Vendors are thus necessarily involved in training efforts for election personnel and poll workers.

Fifth, several workshop participants commented on the incompleteness of testing of electronic voting equipment by vendors and ITAs, which—by assumption—do not address needs or issues that are specifically local. For example, paper trails attached to voting systems must be generated by a printer. Often these printers use thermal paper—but voting records printed on thermal paper may not last as long as is required by local law. Some officials at the workshop noted that they would have preferred to undertake their own testing but that resource constraints (money, personnel, and time) prevented them from doing so. Given the complexity of systems, the quantity of patches, and the variety of ballot positions and configurations to test, it is not clear that electronic voting machines can be adequately tested before being deployed.

Sixth, election jurisdictions vary widely in their knowledge and expertise regarding electronic voting.[20] Those with less knowledge about technology or with less experience in contracting with technology vendors clearly operate at a disadvantage in preparing for the November elections, and a lack of technology background or contracting experience regarding assessments of quality, performance, and reliability can increase the influence of politics and personal relationships in the procurement process. Election officials in such jurisdictions could benefit from their more experienced colleagues in learning about problems associated with the products of different vendors, solutions to such problems, jurisdiction-appropriate contract provisions, backup procedures and contingency plans, and law and regulation. In addition, it is simply a fact that, viewed in the large, electronic voting systems are a relatively new arrival on the election scene, and few jurisdictions can claim to have a great deal of experience with such systems.

Finally, advocacy groups have gained considerable influence in the debate regarding electronic voting. Many of these groups focus on security issues[21] and play an increasingly important role in focusing public attention on the conduct of elections and in stimulating state legislative action intended to mitigate security risks.

[20] See *Asking the Right Questions*, p. 118.

[21] For a more extended discussion of security issues raised by some advocacy groups, see *Asking the Right Questions*, pp. 57-82.

RECOMMENDATIONS

As the November 2006 elections approach, the committee's first and most urgent recommendation is that **election jurisdictions should—indeed must—ensure the availability of backup mechanisms and procedures for use in the event of any failure of e-voting equipment or related technology.** This recommendation is based on the fact that any "flash" cutover to new technology (such as we are seeing today with many e-voting systems) almost guarantees surprises and unintended consequences (e.g., system crashes, unacceptably slow performance). And, although unlikely if appropriate pre-election testing has been undertaken, election officials would be unwise to completely ignore the possibility of problems severe enough to prevent the effective use of the entire system for some period of time on Election Day.

Most organizations have learned the hard way that it is necessary to develop, test, evaluate, and iterate with small-scale prototypes before committing themselves to an organization-wide program of technology upgrade. They have also learned that they should plan on the simultaneous availability of both old and new systems for some period of time, so that failures in the new system do not leave them unable to perform their mission.

Mostly as the result of resource constraints, most election jurisdictions are not (and have not been) in a position to ask vendors for small-scale testing of prototypes in an operational environment before committing to large-scale deployment. Accordingly, jurisdictions must have backup and contingency plans in place that anticipate a wide range of failure conditions, including failures in the middle of the voting process on the day or days of voting.

The committee does not make a specific recommendation on the precise nature of the appropriate backup plans, as these will vary from jurisdiction to jurisdiction. Moreover, there are budgetary constraints on the comprehensiveness of any contingency plan that can be put into place—jurisdictions may only be able to plan for relatively modest problems, such as local system failures in individual precincts, rather than for widespread failures on Election Day.

For risks to system operation involving individual polling places, one option might be for all precincts to have available the location of a number of other precincts to which voters might be redirected. Another option might be to have available and on call technicians and/or a few spare voting machines in a van that could be redeployed promptly. A third option is to ensure that a reasonable stock of hand-countable paper ballots is created before the election and designated for use only in an emergency that renders the original voting method unusable. With preprinting of such ballots, election administrators would have a much easier time accounting for any hand-countable ballots that were produced and/or used.[22] Counting paper ballots is discussed in Appendix C.

---

[22] Still another alternative is to create paper ballots on short notice by making arrangements with a printing firm to use special-purpose ballot stock paper, which would make ballots easier to reconcile as compared to regular stock. Rush jobs to print ballots on Election Day are subject to many potential difficulties, however, such as the drying time for the ink used to print ballots. To the extent that emergency ballots can be created ahead of time without the pressure of immediate (same-day) delivery, many

To prepare for the possibility of widespread failures (i.e., voting systems made inoperable on a large scale, whether by technology or acts of nature), election officials need to engage in a contingency planning process focused on such a possibility.[23] Almost certainly, the choices would be choices among bad alternatives, each one disenfranchising voters to some extent. Primaries and elections for local offices, at least, have been postponed following external disasters, as was done in New Orleans in the aftermath of Hurricane Katrina and in New York City following the 9/11 attacks on the World Trade Center.

Apart from this primary and urgent recommendation, the committee urges that to the extent possible, **jurisdictions should band together in their interactions with vendors.** With 9,500 election jurisdictions in the nation and only a handful of major electronic voting system vendors, it is clear that the leverage of jurisdictions vis-à-vis vendors would be increased significantly if they could present their requirements collectively, for example as part of a negotiating consortium. Even if not, informal information sharing (e.g., about what a vendor is willing to do for one jurisdiction) can support efforts at moral suasion to persuade vendors to be more accommodating to jurisdictions' needs.

Election officials should also seek information from their colleagues about problems associated with the products of different vendors, solutions to such problems, jurisdiction-appropriate contract provisions, backup procedures and contingency plans, and legal and regulatory options. Since jurisdictions are generally not in a position to undertake such research themselves, they might request such assistance from the Election Assistance Commission and other entities in developing a national clearinghouse and resource for information regarding election administration. For example, these organizations could compile best practices related to contracting with vendors for e-voting equipment and related services, develop a database of state election laws to facilitate easy comparisons and information exchange, and establish discussion forums for election officials in which problems and solutions could be discussed candidly.

Finally, **jurisdictions should consider engaging in parallel testing of their voting systems on Election Day if it is feasible to do so.** In parallel testing, some

---

such problems can be avoided.

[23] A few examples can be cited of contingency/threat planning related to elections and elected bodies. For example, Dana Debeauvoir, from Travis County, Texas, produced a report about a planning process that was honored by the Election Center in 2005 (the package of papers is at http://electionupdates.caltech.edu/2005/12/election-center-2005-professional.html). A second example is provided by Oregon, whose state election code requires that each county election official file an elections security plan annually with the Secretary of State. The plan is supposed to include a presentation of security procedures. Third, the Continuity of Government Commission has addressed the issue of ensuring that the Congress could reconstitute itself quickly in the aftermath of a large-scale terrorist attack that killed or incapacitated a large number of senators and/or representatives (see http://www.continuityofgovernment.org/report/report.html). However, none of these efforts specifically address the question of contingency planning for Election Day mishaps.

randomly chosen systems are taken out of service and used instead in a simulated, videotaped "election." Pre-scripted votes are entered as they would be if the machines were in actual use, but since these votes are known, the final vote counts can be checked for accuracy. The committee understands that many jurisdictions will not be able to undertake parallel testing in November 2006 because of time and resource constraints, but to the extent that such testing can occur, it would help to inform others for the 2008 election, and if successful, might help bolster confidence in it as well.[24] This recommendation holds for all jurisdictions that do not use hand-counted paper ballots, but it is particularly important for jurisdictions that use DRE systems not equipped to generate paper trails.

CONCLUSION

Throughout its deliberations and meetings since the start of this study in 2004, the committee has been struck by the dedication and talent of the election officials who have testified. Indeed, these individuals can be regarded as unsung heroes who have kept the machinery of American democracy operating in the face of sometimes overwhelming difficulties. But the November 2006 elections pose challenges like no other previous one regarding reliability, usability, security, training, education, and testing. More jurisdictions than ever before will have electronic voting systems in their polling places. Most importantly, the waiver available for the November 2004 election and provided by HAVA—which allowed states accepting funds for replacing punch card and lever voting systems to postpone replacement until January 1, 2006—has expired. In addition, the November elections appear at this point to be very close, and control of the House or Senate might rest on the outcome of a few close races whose results could be disputed.

However, these observations are not meant to suggest that there will be widespread failures of electronic voting systems, that election results will be clouded by excessive voter confusion about using new electronic voting systems, or that electronic election fraud will necessarily occur in November. Nevertheless, the circumstances of the November election raise the stakes for conducting elections that are regarded as fair and that can withstand close scrutiny even in the face of unproven technology and new election procedures. The challenges facing election officials and the nation in the upcoming election are formidable indeed, and only time will tell if election officials across the land will be able to succeed in the face of these challenges.

Respectfully submitted,

Dick Thornburgh and Richard Celeste, *Co-chairs*
Committee on a Framework for Understanding Electronic Voting

[24] For some additional discussion on parallel testing, see *Asking the Right Questions*, pp. 78-79. Note also that parallel testing itself must be undertaken carefully in order to minimize the possibility that test votes and real votes might be mistakenly intermingled.

APPENDIX A

MEMBERS OF THE COMMITTEE ON

A FRAMEWORK FOR UNDERSTANDING ELECTRONIC VOTING

DICK THORNBURGH, Kirkpatrick & Lockhart Nicholson Graham, LLP, *Co-chair*
RICHARD CELESTE, President, Colorado College, *Co-chair*
R. MICHAEL ALVAREZ, California Institute of Technology
THOMAS SHERIDAN, Massachusetts Institute of Technology (retired)
JOSEPH A. SMIALOWSKI, Freddie Mac
ANTHONY STEVENS, State of New Hampshire
PETER WEINBERGER, Google Inc.

Staff

HERBERT S. LIN, Senior Scientist and Study Director
KRISTEN BATCH, Research Associate
DAVID PADGHAM, Associate Staff Officer
BRANDYE WILLIAMS, Staff Assistant

APPENDIX B

LIST OF PARTICIPANTS IN THE MAY 12, 2006, WORKSHOP OF THE COMMITTEE ON A FRAMEWORK FOR UNDERSTANDING ELECTRONIC VOTING

Doug Chapin, Electionline.org
Donetta Davidson, U.S. Election Assistance Commission
Scott Doyle, Larimer County, Colorado
Eric Fischer, U.S. Congressional Research Service
George Gilbert, Guilford County, North Carolina
Gracia Hillman, U.S. Election Assistance Commission
Susan Inman, Pulaski County, Arkansas
Linda Lamone, Maryland State Board of Elections
Ray Martinez, U.S. Election Assistance Commission
Conny McCormack, Los Angeles County, California
Wendy Noren, Boone County, Missouri
Rene Peralta, National Institute of Standards and Technology
Ion Sancho, Leon County, Florida

APPENDIX C

ON THE MANUAL COUNTING OF PAPER BALLOTS

Counting paper ballots is inherently manual, but there are better and worse ways of doing it. One common method is based on ballot reading and tally marks. One member of a two-person team reads the ballot, declaring those legal votes apparent from the voter's marks. The second team member places a mark on his/her tally sheet for the candidate receiving a vote. This method involves the possibility of a mistake because the ballot is examined only once or a mistake because only one person is doing the tallying. Since this method commonly involves reading through the entire ballot, the ballot reader's eye and brain are not focused on looking for a single type of data, and thus the reader must expend mental effort to distinguish among the contests in which choices are made.

At least one state (New Hampshire), in its state recounts, has been using another process that seems to be less subject to error. This process, based on the use of ballot sorting and piles, involves one member of a two-person team picking up the ballots and placing them in piles corresponding to each choice in a particular race. The other team member observes each ballot as it is placed in a pile. After the sorting process is complete, one team member counts each pile in stacks of 25 and then the other team member recounts each stack. This process enables at least two persons to simultaneously examine each ballot at least once, and to keep things simple by identifying choices in a single race at a time. If one person makes a mistake, the other can catch it. This method is often modified so that each ballot is rechecked during the stack-counting process. Hence, each ballot can be seen two times by each member of the team, for a total of up to four views of each mark on a ballot in each race. The ballot sorting and pile method, which involves as many examinations of the same ballot as there are contests, is noticeably faster than the ballot reading and tally mark approach.

McClatchy Washington Bureau

Print This Article

Posted on Tue, Mar. 24, 2009

Most electronic voting isn't secure, CIA expert says

Greg Gordon | McClatchy Newspapers

last updated: March 24, 2009 04:27:14 PM

WASHINGTON — The CIA, which has been monitoring foreign countries' use of electronic voting systems, has reported apparent vote-rigging schemes in Venezuela, Macedonia and Ukraine and a raft of concerns about the machines' vulnerability to tampering.

Appearing last month before a U.S. Election Assistance Commission field hearing in Orlando, Fla., a CIA cybersecurity expert suggested that Venezuelan President Hugo Chavez and his allies fixed a 2004 election recount, an assertion that could further roil U.S. relations with the Latin leader.

In a presentation that could provide disturbing lessons for the United States, where electronic voting is becoming universal, Steve Stigall summarized what he described as attempts to use computers to undermine democratic elections in developing nations. His remarks have received no news media attention until now.

Stigall told the Election Assistance Commission, a tiny agency that Congress created in 2002 to modernize U.S. voting, that computerized electoral systems can be manipulated at five stages, from altering voter registration lists to posting results.

"You heard the old adage 'follow the money,' " Stigall said, according to a transcript of his hour-long presentation that McClatchy obtained. "I follow the vote. And wherever the vote becomes an electron and touches a computer, that's an opportunity for a malicious actor potentially to . . . make bad things happen."

Stigall said that voting equipment connected to the Internet could be hacked, and machines that weren't connected could be compromised wirelessly. Eleven U.S. states have banned or limited wireless capability in voting equipment, but Stigall said that election officials didn't always know it when wireless cards were embedded in their machines.

While Stigall said that he wasn't speaking for the CIA and wouldn't address U.S. voting systems, his presentation appeared to undercut calls by some U.S. politicians to shift to Internet balloting, at least for military personnel and other American citizens living overseas. Stigall said that most Web-based ballot systems had proved to be insecure.

The commission has been criticized for giving states more than $1 billion to buy electronic equipment without first setting performance standards. Numerous computer-security experts have concluded that U.S. systems can be hacked, and allegations of tampering in Ohio, Florida and other swing states have triggered a campaign to require all voting machines to produce paper audit trails.

The CIA got interested in electronic systems a few years ago, Stigall said, after concluding that foreigners might try to hack U.S. election systems. He said he couldn't elaborate "in an open, unclassified forum," but that any concerns would be relayed to U.S. election officials.

Stigall, who's studied electronic systems in about three dozen countries, said that most countries' machines produced paper receipts that voters then dropped into boxes. However, even that doesn't prevent corruption, he said.

Turning to Venezuela, he said that Chavez controlled all of the country's voting equipment before he won a 2004 nationwide recall vote that had threatened to end his rule.

When Chavez won, Venezuelan mathematicians challenged results that showed him to be consistently strong in parts of the country where he had weak support. The mathematicians found "a very subtle algorithm" that appeared to adjust the vote in Chavez's favor, Stigall said.

Calls for a recount left Chavez facing a dilemma, because the voting machines produced paper ballots, Stigall said.

"How do you defeat the paper ballots the machines spit out?" Stigall asked. "Those numbers must agree, must they not, with the electronic voting-machine count? . . . In this case, he simply took a gamble."

Stigall said that Chavez agreed to allow 100 of 19,000 voting machines to be audited.

"It is my understanding that the computer software program that generated the random number list of voting machines that were being randomly audited, that program was provided by Chavez," Stigall said. "That's my understanding. It generated a list of computers that could be audited, and they audited those computers.

"You know. No pattern of fraud there."

A Venezuelan Embassy representative in Washington declined immediate comment.

The disclosure of Stigall's remarks comes amid recent hostile rhetoric between President Barack Obama and Chavez. On Sunday, Chavez was quoted as reacting hotly to Obama's assertion that he's been "exporting terrorism," referring to the new U.S. president as a "poor ignorant person."

Questions about Venezuela's voting equipment caused a stir in the United States long before Obama became president, because Smartmatic, a voting machine company that partnered with a firm hired by Chavez's government, owned U.S.-based Sequoia Voting Systems until 2007. Sequoia machines were in use in 16 states and the District of Columbia at the time.