Review of FVAP's Work Related to Remote Electronic Voting for the *UOCAVA* Population

29 December 2015

The estimated cost of this report or study for the Department of Defense is approximately $306,000 in Fiscal Years 2014 - 2015. This includes $284,000 in expenses and $22,000 in DoD labor.

Generated on 2015Dec15 RefID: C-44CC8BA

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The United States is a highly mobile society and many U.S. citizens live, work, and study abroad. Uniformed Services personnel, and their families, are often called upon to live outside their State of residence, and oftentimes are stationed abroad. Recognizing that absent members of the military, their families and U.S. citizens living abroad face unique challenges to participating in U.S. elections, Congress created a set of protections to make voting in federal elections easier and more accessible. These protections are codified in the *Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)*.

FVAP has a long history of conducting research on barriers to absentee voting and working with States to determine how these hurdles can be reduced or eliminated. In 2000, FVAP conducted a Voting Over the Internet (VOI) pilot project that intended to address the specific needs of the military when attempting to vote absentee remotely. Although the VOI pilot was limited in scope and participation, Congress recognized the initial success and mandated the conduct of an electronic voting demonstration project through the National Defense Authorization Act (NDAA) for Fiscal Year 2002 (FY 2002) for a statistically relevant population of absent Uniformed Service personnel. Although the term "statistically relevant" is an undefined term for the size of such a project, FVAP recognized the need for an expanded approach for conducting absentee voting over the Internet for the 2004 General Election. In 2004, FVAP's attempt to execute this project was canceled by the Deputy Secretary of Defense "over the inability to ensure legitimacy of votes that would be cast."

In the Ronald W. Reagan NDAA FY 2005, Congress maintained the requirement for FVAP to conduct this initiative, but offered authority for FVAP to wait for the adoption of standards by the newly formed United States Election Assistance Commission (EAC) prior to conducting the "electronic voting demonstration project" (i.e., remote Internet voting) for *UOCAVA* citizens. This authority authorized a window of opportunity for system development from the date the standards were adopted until the following general election – a period of less than two years.

In 2010, the EAC adopted the *UOCAVA* Pilot Program Testing Requirements (UPPTR) which addressed the standards for the conduct of a pilot program consisting of kiosks (e.g., polling stations) at various locations around the world with the ability to provide a paper audit record of each vote cast. These criteria were used by FVAP to consider the possible approach for fulfilling the requirements of the electronic voting demonstration project.

As an alternative strategy to a kiosk approach, FVAP also considered leveraging commercially available Internet voting systems to speed the time for deployment and increase the likelihood of success for meeting Congressional intent. FVAP examined systems offered by Internet voting system providers registered with the EAC at the time of the research.

FVAP's primary research and deliberation focused on answering a series of policy questions that reflected the changing information assurance environment for the Internet and reflected a series of broad consensus topics gathered during a joint meeting conducted by the EAC, FVAP and the National Institute of Standards and Technology (NIST) in August 2010. (In the NDAA FY 2015, Congress eliminated the requirement for FVAP to conduct the electronic voting demonstration project. With the repeal of the requirement, DoD is no longer exploring program implementation in this area.)

Table 1.1 below details the fundamental research questions driving FVAP's research surrounding the electronic voting demonstration project:

Table 1.1: Research Questions and Deliverables Addressing System Integrity and Security

Research Question	Primary Research Deliverables
What type of FVAP-sponsored conformance test should be used to accredit these systems against the *UOCAVA* Pilot Program Testing Requirements (UPPTR)? What is the impact of this conformance test against the timeline for implementing a remote kiosk-based approach?	• Recommendations for the UPPTR • Voting System Testing Laboratory Functionality and Security Testing
What is the level of resistance existing systems possessed against penetrations? What is the eventual type of approach and methodology FVAP should consider for a large-scale implementation of a penetration test as part of its security posture?	• Penetration Testing of a Simulated Election
Would the advent of software assurance tools hold value for identifying the extent of known defects in software source code? Could these tools be used to assist with source code reviews? What is the extent of coverage that software assurance tools could provide?	• Investigation of the use of Software Assurance Tools on Internet Voting Software Applications

Additionally, FVAP conducted a set of studies related to the e*nvironment* in which any remote electronic voting demonstration project would occur. FVAP examined issues related to the use of DoD assets – specifically, its public key infrastructure (e.g., Common Access Card) and the secure U.S. Government Non-classified Internet Protocol Router Network (NIPRNet) – to fulfill the electronic voting demonstration project requirement. FVAP also considered whether remote kiosk voting was a viable model for remote electronic voting. Both analyses identified key barriers that would have to be addressed before either DoD infrastructure or kiosks were used as part of remote electronic voting initiatives. The specific research questions are linked to research deliverables listed in Table 1.2.

Table 1.2: Research Questions and Deliverables Addressing the System Environment

Research Question	Research Deliverable
What are the relative benefits/concerns with using the Defense Information Systems Network (DISN) as part of the overall architecture? Could the Department consider the use of a standardized client configuration as part of its remote electronic voting system? What would be the supporting logistics associated with this?	• Voting Over the DISN-CAC Analysis Feasibility Evaluation
What is the role of the Department's Common Access Card (CAC) for system authentication purposes? What is the potential for its use as part of the voter authentication process?	• Voting Over the DISN-CAC Analysis Feasibility Evaluation
What is the supporting statutory and legal framework for the States to participate in a remote kiosk-based pilot?	• The 2008 Okaloosa Distance Balloting Pilot Project

Finally, FVAP conducted research that considers the overall risk environment in which any remote electronic voting demonstration project would be fielded. The goal of this research was to determine if there was an effective process by which the risk environment could be defined and then those defined risks could be quantified. The specific research questions are linked to the research deliverable found in Table 1.3.

Table 1.3: Research Questions and Deliverables Addressing Quantifiable Comparative Risk

Research Question	Research Deliverable
What is the comparative level of risk between the existing postal-based system and that of a remote electronic voting system? Can this risk be quantified?	• Comparative Risk Analysis of the Current *UOCAVA* Voting System and an Electronic Alternative

The tools developed as part of the comparative risk analysis are intended to be built upon and refined over time as part of an active consensus building process. These tools could be used by the election community as the basis for testing an Internet voting system threat matrix, recognize relative risk for the existing postal system versus an Internet-based system or use the tool to recognize particular tradeoffs during system development.

CONCLUSIONS AND RECOMMENDATIONS

FVAP's work related to remote electronic voting was driven by congressional requirements that existed at the time. The enactment of its first requirement to conduct an electronic voting demonstration project opened up a new research agenda for FVAP. In addition to meeting its core

mission to ensure that Service members, their eligible family members, and overseas citizens are aware of their right to vote and have the tools and resources to successfully do so, FVAP began to identify how it could meet the electronic voting demonstration project requirement for these voters.

FVAP intends the conclusions below to be a cohesive set of findings and any actions taken based upon them should reflect all of the conclusions and not any single conclusion by itself.

- Any potential remote electronic voting pilots conducted with involvement from DoD or other federal agencies need to consider the balance between federal and State roles. The current information security environment is such that specific roles and system owners need to be defined upfront in the event an intrusion occurs that calls the integrity of voted absentee ballots cast by *UOCAVA* citizens into question.
- A remote kiosk voting system, under present laws and conditions, is not a tenable solution for serving the *UOCAVA* population through current Departmental regulations.
- The software assurance tools used as part of this initiative successfully tested and identified software defects as true positives. The use of multiple tools added marginal value to the number and scope of positive defects, but more research is required on the exact combination of tools that yield the most effective level of detection. It is important to note that merely identifying defects does not provide an overall assessment of a system's security posture. Rather, the identification of defects necessitates a deeper level of code examination to determine the true nature of the risk and context.
- Further research should examine the use of software assurance tools for voting systems and their long term ability to increase the quality of the software and increase confidence levels that existing software is free of known defects.
- Comparative risk analysis – and an appreciation of the risk environment – is critical for the success of any remote electronic pilot as it will drive not only a consensus approach to understanding the inherent threats through a consensus approach, but it will also inform the potential tradeoffs that should occur when considering system development in order to inject no more significant risks than the existing system. A comparative risk analysis should involve an array of computer security and election administration experts and should be seen as a means to provoke active discussion and collaboration.
- Any remote electronic voting pilot will take time to implement; two years is not an adequate period to test, remediate, and field such a system. The research conducted by FVAP found that, before any remote electronic voting pilot is fielded, the system should undergo extensive risk assessment modeling, including voting system standards testing, software assurance testing, penetration testing, usability testing, and conformance testing.

The research and conclusions listed above have the following specific implications for FVAP moving forward:

- FVAP can best serve its constituency by focusing on its core mission. FVAP has three primary objectives: (1) informing *UOCAVA* citizens of their right to vote and assisting them as they exercise their right to vote, (2) assisting the States in complying with relevant federal laws by providing current information, and (3) working with State and local election officials on behalf of *UOCAVA* voters to identify impediments to their ability to exercise their right to vote, and methods to overcome those impediments.

- Should the EAC and NIST decide to apply this research to their standards development process, FVAP would be able to provide additional background information regarding the research it has already conducted to help these agencies.

As noted, the NDAA (FY 2015), Congress eliminated the requirement for FVAP to conduct the electronic voting demonstration project. With the repeal of the requirement, DoD is no longer exploring program implementation in this area. However, with the level of investment through the use of public funds and the length of time associated with the original demonstration project requirement, FVAP believes that the research, associated tools, and identification of the outstanding questions are valuable and should be shared with the *UOCAVA* stakeholder community. Should a State determine it wishes to pursue a full Internet voting solution, it should do so in a fashion that takes advantage of the knowledge gleaned from these extensive research efforts. A State proceeding without a carefully constructed plan to mitigate information security risks and apply stringent security standards increases the potential for failure either in terms of its technical implementation, security posture or resulting voter confidence.

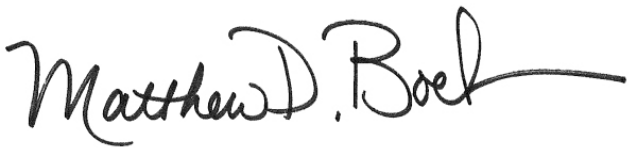
MESSAGE FROM THE FVAP DIRECTOR

It is my distinct pleasure to present the Federal Voting Assistance Program's (FVAP) report on its *Electronic Voting Demonstration Project Research*. The research described in this report was conducted to inform the project planning and execution of the Department of Defense's (DoD) previously mandated electronic voting demonstration requirement. In the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act (NDAA) for Fiscal Year 2015, Congress eliminated this requirement and DoD is no longer exploring program implementation in this area. However, I believe the research and identification of outstanding questions are valuable and should be shared with the *Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)* stakeholder community. The issues surrounding voting and the use of the Internet will not be going away anytime soon; I hope this research helps facilitate a constructive dialogue.

Due to its legislative requirement first established in the NDAA FY 2002, FVAP embarked on an ambitious research agenda to understand the pros and cons surrounding the issue of Internet voting and its potential for supporting *UOCAVA* voters. Prior to moving headlong with the development of a system architecture, FVAP wanted to understand the implications of such technology in a world that reflects an ever-changing information security environment. This report explains the context of the research associated with the electronic voting demonstration project, and discusses the scope and purpose of the research, its limitations, conclusions and recommendations.

Each reader should be aware there is no definitive recommendation on the use of Internet voting over the long-term. However, much of the supporting research may hold value for any future deliberations on the merits of remote electronic voting. While FVAP remains committed to providing overall voting assistance, the questions raised in this research revealed the importance for FVAP to focus on its core mission of voter assistance and work within the larger election community and facilitate a greater understanding of the *UOCAVA* voter experience.

With the repeal of the requirement, FVAP is able to focus on its core mission to ensure that Service members, their eligible family members, and overseas citizens are aware of their right to vote and have the tools and resources to successfully do so from anywhere in the world. This report should not be used to convey a position in support or against States moving forward with such technology; it is important to remember that FVAP neither advocates for nor against Internet voting. It is my intention that by sharing this research with the *UOCAVA* community, stakeholders can take advantage of the knowledge gleaned from FVAP's experiences and these extensive research efforts.



SECTION 1: VOTING, *UOCAVA* VOTING, AND THE INTERNET

Since the Civil War, State and Federal officials have worked to determine how to ensure that military personnel engaged in service to their country can participate in elections. Many of the election reforms that we have today – e.g., in-person early voting, absentee voting – have their origins in efforts to enfranchise Union soldiers who were engaged in conflict at the time of the 1864 election.[1] The obvious problem for military personnel who are serving their nation while stationed far from home is that they cannot easily get to their usual voting precinct in the State in which they are registered to vote in order to cast their ballot in elections.

The military voting problem became more complex in the 20th century. The military went from being largely organized by State militias, as it had been previously, to being an integrated force where individuals from across the United States were in the same units. State election officials could no longer know that all military personnel from their State would be located together in a given area during their service. Additionally, large-scale mobilizations occurred, sending millions of Service members abroad to serve for extended durations, oftentimes in remote and difficult-to-access locations. More recently, concerns have widened to include a broader population of U.S. citizens who are overseas during elections, including those who reside abroad.

Similar issues have arisen as U.S. civilians have traveled or moved abroad. This mobility to other nations can occur when U.S. citizens are dependents of Armed Forces members who are stationed abroad, or because they are employed by the Federal Government and work overseas. Other U.S. citizens are abroad because they are studying in another nation, working as a missionary, their employer has sent them overseas, or because they have decided to live outside the U.S. In each of these situations, these non-military U.S. citizens located overseas also may have difficulty obtaining their voting registration and balloting materials in order to effectively exercise their right to vote in U.S. elections.

Extended distances and more complex organizational arrangements create unique challenges for State and Federal officials as they work to effectively serve these various types of voters who are abroad. In order to coordinate the efforts to serve these military personnel, their family members, and other U.S. citizens abroad, the *Uniformed and Overseas Citizens Absentee Voting Act* (*UOCAVA*) was signed into law in 1986 to provide registration and voting assistance to these citizens away from home (52 USC §203). In 1988, Presidential Executive Order 12642 named the Secretary of Defense as the Designee charged with administering *UOCAVA*. Further, Department of Defense Instruction 1000.04, Federal Voting Assistance Program, assigns the Under Secretary of Defense for Personnel and Readiness as the Presidential designee; the responsibilities are carried out by the Director of FVAP. Under these authorities, FVAP provides voter registration and voting information to those eligible to vote in applicable U.S. elections.

[1] There are a number of recent studies of the history of UOCAVA and military voting: R. Michael Alvarez, Thad E. Hall, and Brian Roberts, "Military Voting and the Law: Procedural and Technological Solutions to the Ballot Transit Problem," *Fordham Urban Law Review*, XXXIV, 3 (2007): 935-996. Bruce E. Cain, Karin MacDonald, and Michael H. Murakami, "Administering the Overseas Vote," *Public Administration Review*, 66, 5 (2008): 802-813. Donald S. Inbody, "Political Barriers to Military Voting: A Brief Historical Overview," *OVF Research Newsletter*, 2, 3 (2008), 1-4. Donald S. Inbody, "Voting by Overseas Citizens and Military Personnel," Election Law Journal, 14, 1 (2015), 54-59.

In 2009, *UOCAVA* was amended by the *Military and Overseas Voter Empowerment* (*MOVE*) *Act* (Subtitle H of P.L. 111-84, National Defense Authorization Act for Fiscal Year 2010). The *MOVE Act* required that States provide enhancements to ballot delivery, undertake efforts to improve voter assistance, and that FVAP develop a comprehensive web portal with Internet-based tools to guide voters through the absentee voting process. All of these refinements were intended to make the process of voting and registration easier for *UOCAVA*-covered citizens.

UOCAVA ensures that voting assistance is provided to U.S. citizens who are:

- Active members of the Armed Forces, the Merchant Marines, and their eligible family members;
- The commissioned corps of the Public Health Service, the National Oceanic and Atmospheric Administration, and their eligible family members;
- U.S. citizens residing outside the United States.[2]

Recent research sponsored by FVAP estimates that in 2010 there were 4.3 million U.S. civilians living abroad.[3] Current estimates from the Department of Defense (DoD) indicate there are approximately 1.4 million members of the Armed Forces.[4] This implies that there are as many as 5.7 million U.S. citizens who fall within the protections of *UOCAVA* and its related legislation.

The Ballot Transit Time Problem

Starting in World War I, and continuing through World War II and today, the primary solution that has been offered for enfranchising *UOCAVA* voters has been postal registration and postal voting. Today, the postal voting process starts with the potential voter sending a registration form or a ballot request to the appropriate election official. If the voter is deemed eligible to vote in the jurisdiction, the ballot and associated material are sent to the voter by the local election official. The voter marks the ballot, puts the marked ballot in an envelope, and mails the ballot back to the local election official.

UOCAVA postal voters can experience what is commonly referred to as a "ballot transit time" problem. This problem reflects that, for *UOCAVA* voters, their Federal Post Card Application (FPCA) and their ballot have to travel farther and will be handled by multiple postal services. For example, U.S. civilian voters living in Germany will have their ballots handled by the U.S. Postal Service (USPS) and Deutsche Post both on the way to them and on the way back to their local election official (LEO). A U.S. Army soldier stationed at a base in Germany will have his or her postal ballot handled by the USPS and the Military Postal Service Agency (MPSA) in both directions. The time it takes a ballot to travel to and from overseas military personnel can vary based on where they are stationed; for

---

[2] This definition is from the FVAP website, paraphrased from "Registration and Voting by Absent Uniformed Services Voters and Overseas Voters in Elections for Federal Office," 52 USC §20310, January 7, 2011. Retrieved from http://www.fvap.gov/info/laws/uocava

[3] See Table 7 in Fors Marsh Group LLC, "A Model for Developing Estimates of U.S. Citizens Abroad: Final Technical Report." July 23, 2013. Retrieved from https://www.fvap.gov/uploads/FVAP/Reports/OCE_Technical_Report.pdf

[4] U.S. Department of Defense, Defense Manpower Data Center. "Active Duty Military Personnel by Service by Region/Country (Updated Quarterly)." October 31, 2014. Retrieved from https://www.dmdc.osd.mil/appj/dwp/dwp_reports.jsp.

example, personnel based on a ship, a military installation, a non-combat area, and a forward combat area will all face different ballot transit time issues.

The ballot transit time problem has been studied by numerous organizations, including the Government Accountability Office (GAO), the U.S. Department of Defense Inspector General, and the Pew Charitable Trusts. The general consensus of studies done on the topic is that ballot transit problems can make it difficult for *UOCAVA* voting to be successful. For example:

- In 2001, the GAO found that transit times for first class mail could be from five days to a month. They also found that almost two-thirds of all disqualified absentee ballots were rejected because election officials received them after the official deadline.
- A 2004 GAO study found that ballot transit times to Iraq in 2003 were between 12 to 18 days for mail sent from the United States into Iraq, but 25% of test letters were delivered more than 18 days after the date mailed. Mail transit from Iraq to the United States took more than 18 days for two of the six months of the evaluation. These transit times meant that it would be very difficult for mail to be sent and returned from Iraq in less than 30 days, a typical deadline lead time for absentee ballots to be sent to prospective voters.
- The Pew Charitable Trusts' 2009 *No Time to Vote: Challenges Facing America's Overseas Military Voters* study found that in 16 States and the District of Columbia, the date for sending a ballot to *UOCAVA* voters did not allow for enough time for a ballot to get from a LEO to the voter and back to the LEO. This study was influential in the passage of the *MOVE Act*.

In addition to the actual transit time problem, a related issue is that the distance between the *UOCAVA* voter and LEO makes it difficult for any problem associated with the voting process to be easily remedied. For example, if a U.S.-based voter registers to vote and there is a problem with the registration – e.g., the voter fails to sign the registration, a part of the form is illegible – the LEO can contact the voter by phone or by mail and the problem can be resolved in a relatively short time frame. However, the same problems on an FPCA are more difficult to address because recontacting the voter and receiving a reply via mail can take weeks, not days.[5]

The ballot transit time problem is very hard to tackle without changing the means by which election materials are transmitted. The advent of the Internet provided an opportunity to introduce a new transmittal method.

Overcoming the Ballot Transit Time Problem: The Internet

The Internet has changed how people view social relations. One quite common view expressed at the outset of widespread Internet use was that "Perhaps more than any other distance media, the

[5] There are other issues with postal voting that have received the attention of researchers. First, ballots cast via postal voting have higher residual vote rates than ballots cast in person using technologies that can correct for common mistakes (R. Michael Alvarez, Dustin Beckett, and Charles Stewart III. "Voting Technology, Vote-by-Mail, and Residual Votes in California, 1990-2010," *Political Research Quarterly*, 66, 3 (2013), 658-670. In postal voting, ballots are outside the usual chain of custody associated with in-person voting, thus introducing a variety of concerns regarding the potential for coercion and fraud (R. Michael Alvarez and Thad E. Hall, "Building Secure and Transparent Elections Through Standard Operating Procedures," 2008, *Public Administration Review*, 68(5), 828-838).

Internet and the Web help overcome the barriers of time and space…"[6] This attribute of the Internet has obvious implications for addressing the ballot transit time problem for *UOCAVA* voters, since this problem is one of serving a population (the voter) separated by time and distance from their service provider (the LEO). The political, technology, and academic communities recognized the possibilities – as well as possible problems – of the Internet in the voting process.[7] Two of the most prominent initial reports published addressing these questions were the National Science Foundation's *Report of the National Workshop on Internet Voting: Issues and Research Agenda*.[8] (Arlington, Virginia: March 2001) and the California Internet Voting Task Force's *A Report On the Feasibility of Internet Voting* (Sacramento, California: January 2000).

Although these reports varied in their recommendations as to whether Internet voting was actually feasible given security concerns related to Internet-based transactions, there was a general consensus that the Internet was a technology that addressed the ballot transit time problem. Voter registration and balloting materials could be sent instantaneously to the distant voter, the technology, and any administrative questions that may arise about a voter's materials could be instantly addressed.

FVAP was at the forefront of recognizing that the Internet had the potential to improve voting for its *UOCAVA* voters. The proactive efforts of FVAP were documented by the U.S. Election Assistance Commission (EAC) in its report *A Survey of Internet Voting*:

> By the mid-1990s it became apparent that mail transit time and unreliable postal delivery posed significant barriers for many *UOCAVA* citizens, preventing them from successfully exercising their right to vote. To address this issue, in October 1997 FVAP met with State and local election officials to discuss a project to test the feasibility of using electronic delivery as an alternative to postal mail. The State and Local Government Alliance was established to work with FVAP to plan this effort. By 1999 the groundwork was laid to conduct a small pilot project for the 2000 General Election.[9]

FVAP's work was occurring concurrent with the dot-com boom of the 1990s.[10] The mid-1990s had a growth phase to its development and then a "hype" phase, where Internet use was expanding at rapid rates and the business of e-commerce and how the Internet would change the world were constantly in the news. The work of FVAP was grounded in an understanding that the growth of the

---

[6] This quote comes from the context of distance education. See Sandra Kerka, "Distance Learning, the Internet, and the World Wide Web." *ERIC Digest*, 1996.

[7] A search of Google Scholar (scholar.google.com) finds 152 articles and reports related to Internet voting were published between 1995 and 2000.

[8] National Science Foundation. *Report of the National Workshop on Internet Voting: Issues and Research Agenda*. Arlington, Virginia: March 2001; California Internet Voting Task Force, *A Report on the Feasibility of Internet Voting*. Sacramento, California: January 2000.

[9] U.S. Election Assistance Commission, Voting System Testing and Certification Division. *A Survey of Internet Voting*, (September 41, 2011), 6-7. Retrieved from http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf.

[10] For a brief history of this period, see Steve Case, "Steve Case: The Complete History Of The Internet's Boom, Bust, Boom Cycle." Business Insider, January 14, 2011. Retrieved from http://www.businessinsider.com/what-factors-led-to-the-bursting-of-the-internet-bubble-of-the-late-90s-2011-1

Internet would put more potential *UOCAVA* voters in a position to use the Internet to vote and solve the ballot transit time problem.

Since 1990, FVAP, working with State and local election officials, has engaged in a variety of initiatives to overcome the ballot transit time problem and help the *UOCAVA* population register and vote. These initial efforts culminated in an attempt at fully utilizing the Internet to provide a full absentee voting solution for *UOCAVA* voters during the 2000 election.

Terminology

This report discusses several concepts that are closely related. In order to avoid confusion, each concept is defined here.

Remote Internet Voting is any form of ballot delivery where a voter's ballot selections are returned to a tabulation system via the Internet.

Remote Kiosk Voting is Internet voting conducted from a voting platform provided by sponsor [e.g., a local election office].

Remote Electronic Voting is the submission of a voter's ballot selections over public infrastructure from a location other than a polling place. Remote electronic voting can be performed from systems in controlled and uncontrolled environments. Remote kiosk and remote Internet voting also fit this definition.

Online is used to define a task a person can complete online, such as "register to vote online."

Internet-based is used to describe a *system* that exists online, such as a State's Internet-based voter registration system.

[The definitions of "remote Internet" and "kiosk Internet" and "remote electronic" voting are taken from the EAC's *A Survey of Internet Voting*, pp. 10-11. Retrieved from http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf.

FVAP'S ORIGINAL PILOT: VOTING OVER THE INTERNET

In the 2000 general election, FVAP conducted the Voting Over the Internet (VOI) pilot project as a proof of concept to determine if a remote Internet voting system could be implemented. The following jurisdictions volunteered to participate in this pilot: South Carolina (Statewide); Okaloosa County, FL; Orange County, FL; Dallas County, TX; and Weber County, UT. In all, 84 individuals voted in the pilot, resulting in 83 cast ballots. The pilot allowed voters from these jurisdictions to register to vote, request a ballot and vote over the Internet. In order to participate, potential voters had to contact their LEO to inform them that they wanted to participate, and after properly identifying themselves, voters were issued a digital certificate and an accompanying password.

The VOI project predated the current DoD identification system, the Common Access Card (CAC), which will be discussed in more depth in this report. Instead, the VOI project leveraged the DoD Public Key Infrastructure (PKI) system that was in place in 2000. Voters used the PKI to

authenticate themselves when using the registration and voting system.[11] The process for voting is described in the EAC's *Internet Voting* report:

> After the LEO approved the EFPCA and the voting period began, the voter requested a blank ballot using the same login process described above. When the LEO received this request, they transmitted a ballot to the voter. The voter recorded their selections online and reviewed their choices on a confirmation screen. An affirmation screen appeared for the voter to enter their digital signature password, and then click on the Electronically Sign and Send button to transmit the voted ballot to the LEO. The voter received notification that the LEO successfully received the E-Ballot.[12]

The VOI project had the critical components for a remote Internet voting effort: (1) the ability to register to vote online, (2) the ability to vote online, (3) notification that the ballot was received by the LEO, and (4) a digital identification protocol that allowed voters to "sign" their ballots electronically. This pilot also identified many of the complexities related to managing an Internet voting process from the LEO side, especially those related to integrating each LEO's existing election management system (EMS) with the Internet system for electronic ballot transmission, vote capture, and vote tabulation.

FVAP's VOI initiative was viewed as a successful demonstration of the feasibility of Internet-based registration and voting for *UOCAVA* citizens. The VOI evaluation report summarizes the effort: "The VOI Pilot project was a feasibility study that demonstrated that a stand-alone system for remote registration and voting over the Internet can be a secure, viable alternative to the by-mail process in a small-scale, tightly controlled environment."[13] However, the initiative was only a feasibility study, an attempt to understand whether a fully functional Internet-based system for voter registration and balloting could be developed and implemented in a federal election. It was clear at the time that much more work was needed, and FVAP's VOI evaluation report, which was released in June 2001, concluded with four recommendations:

1. "Implement a broader scale pilot project for remote registration and status checking that is electronically integrated with existing voter registration systems in one to three States for the 2004 General Election."
2. "Continue participation in the development of Internet registration and voting system standards."
3. "Support State legislative initiatives to allow remote registration and voting."

---

[11] The VOI assessment report provides more details regarding the exact procedure used to issue digital certificates to VOI pilot voters, which used the DoD Public Key Infrastructure (PKI): "The issuing procedure for digital certificates required the recipient to appear in person before an issuing authority or the authority's trusted agent and present official photo identification. After receiving and signing the certificate document, the participant had to "fulfill" the certificate by accessing the PKI Web site and downloading his/her certificate to a floppy disk. The participant also had to assign a password to his/her digital certificate." U.S. Department of Defense, Washington Headquarters Services, Federal Voting Assistance Program, *Voting Over the Internet Pilot Project Assessment Report*, June 2001, retrieved from http://www.fvap.gov/uploads/FVAP/Reports/voi.pdf, (1-14).

[12] Election Assistance Commission, *A Survey of Internet Voting*, 37.

[13] Federal Voting Assistance Program, *Voting Over the Internet Pilot Project Assessment Report*, 6-11.

4. "Continue research to identify solutions to outstanding issues to permit the eventual implementation and operational use of a remote registration and voting system."[14]

It is important to note these recommendations because they form the foundation for the congressional mandate in the National Defense Authorization Act (NDAA) for Fiscal Year 2002 (FY 2002) requiring FVAP to conduct a remote electronic voting demonstration project. To satisfy this requirement, FVAP began its research efforts to better understand how new communications technologies such as the Internet could be deployed to mitigate existing problems with the paper-based postal voting systems for *UOCAVA* voters.

SECURE ELECTRONIC REGISTRATION AND VOTING EXPERIMENT (SERVE)

After the VOI project, in 2001 Congress enacted the NDAA for fiscal year 2002. The NDAA FY 2002 authorized FVAP to undertake an electronic voting demonstration project in November 2002 with a "statistically relevant" number of "absent Uniformed Service voters."

Absent Uniformed Services Voter Definition

According to 52 USC §20310, an 'absent Uniformed Services voter means:

(A) a member of a Uniformed Service on active duty who, by reason of such active duty, is absent from the place of residence where the member is otherwise qualified to vote;

(B) a member of the merchant marine who, by reason of service in the merchant marine, is absent from the place of residence where the member is otherwise qualified to vote; and

(C) a spouse or dependent of a member referred to in subparagraph (A) or (B) who, by reason of the active duty or service of the member, is absent from the place of residence where the spouse or dependent is otherwise qualified to vote

Retrieved from: http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title52-section20310&num=0&edition=prelim#sourcecredit

This requirement led FVAP to initiate the Secure Electronic Registration and Voting Experiment (SERVE) project, which would again test the use of remote Internet voting for *UOCAVA* citizens in the 2004 General Election. Building upon the foundation provided by the VOI study, and the recommendations made at the conclusion of that project, SERVE was intended to develop an Internet-based registration and voting system that a sufficiently large number of counties and States would use, resulting in a large number of *UOCAVA* citizens using the system. This broader deployment would facilitate studying many different questions about the deployment of an Internet-based registration and voting solution for *UOCAVA* voters; in particular, how such a voting solution

[14] Federal Voting Assistance Program, *Voting Over the Internet Pilot Project Assessment Report*, 6-12--6-14.

might affect the workflow of State and county election administrators and how it would affect the voting experience of *UOCAVA* citizens. FVAP invited all States to participate and, in the end, 55 counties located in the States of Arkansas, Florida, Hawaii, North Carolina, South Carolina, Utah, and Washington volunteered to participate in this pilot.

SERVE was to allow participating jurisdictions the same four key attributes in communicating with their voters that were present in the VOI project: the ability to register, vote, receive a "vote received" confirmation, and digital signature identification. However, the SERVE system was never implemented. As the EAC report notes, "The SERVE project was cancelled before it was deployed due to security concerns raised by a group of computer scientists. These individuals publicly issued a critique of the system contending that the use of personal computers over the Internet could not be made secure enough for public elections and called for the project to be terminated."[15] It should be noted here that the critique of SERVE was not related to the SERVE system itself but to the security of Internet voting in general.

SERVE involved the potential participation of a wide range of counties and States; it was clear that any large-scale electronic registration and voting project would expose cross-state conflicts because of variations that exist across State and local election administration procedures, laws, and regulations. For example, the issue of integrating each state election management system (EMS) with the Internet registration and voting system remained complicated; each State has its own requirements for ballot design and each EMS also required specific "widgets" to convert its data into a format that could be used by the SERVE system (and converted back). In addition, ensuring that the States – not FVAP or contractors – had ultimate control of the servers used in the project was also a critical issue.

Second, the use of DoD PKI infrastructure (i.e., CAC) would have allowed all military personnel to easily use SERVE. FVAP was in the process of determining how to provide similar authentication to non-military personnel covered by *UOCAVA* at the time SERVE was canceled. Prior to the termination of the SERVE project, the question of how to provide digital identities to potential *UOCAVA* users of the SERVE system who had not been issued a CAC was under active consideration, but remained unresolved. Third, it became clear that the security and integrity of any remote electronic voting system for *UOCAVA* voters needed careful examination, and that research was necessary to identify and mitigate risks to any proposed electronic registration and voting system. Additionally – as was also the case with respect to the VOI project – the need for standards, testing, and certification procedures for an Internet-based registration and voting system arose during the SERVE project. At the time of the SERVE system's development, the lack of standards made it difficult to evaluate whether the registration and voting system then under development would meet any particular set of performance, reliability, accessibility, usability, and security requirements.

Finally, the complexities involved in the development and implementation of a system that might have served a number of States, dozens of counties, and a large number of *UOCAVA* voters pointed out the need for the development of a process that would bring together all key stakeholders to discuss the issues of Internet-based registration and voting and seek consensus on solutions to those issues. Despite the cancellation of the SERVE project, the NDAA FY 2005 reiterated a requirement that FVAP implement the electronic voting demonstration project, but only after

[15] Election Assistance Commission, *Survey of Internet Voting,* 29.

guidelines could be developed for electronic absentee ballots, and after the EAC certified that it will assist the DoD in this effort.

REMOTE KIOSK VOTING

In 2008, Okaloosa County, Florida, implemented the Okaloosa Distance Balloting Project (ODBP), which was a remote kiosk voting pilot. The *UOCAVA* Pilot Program Testing Requirements defines kiosk voting as a voting system with the following four components:

1. A system server which runs the voting software, stores voted ballots, and provides system administration functions;
2. One or more kiosks which are designated remote locations that service multiple election jurisdictions are staffed by kiosk workers who verify voter identity and eligibility, and are equipped with electronic vote capture devices with printing capability.
3. A tabulation device at each participating local election office which decrypts and tabulates the ballots for that jurisdiction; and
4. Communications links that tie the system components together.

The remote kiosk system used in the Okaloosa pilot then had voters digitally sign their ballot, which was then encrypted and transmitted directly to the voting system server. A paper record of the marked ballot was also printed and retained in a secure ballot box, paper records were then later audited against the electronically recorded and transmitted ballots.

The Okaloosa pilot had kiosks at voting sites established in hotels at three overseas locations – Mildenhall, England; Ramstein, Germany; and Kadena, Japan – where there were U.S. military installations with high concentrations of Okaloosa voters. The kiosk process was different from traditional Internet voting because the voters cast ballots in person; the ballots were just transmitted over the Internet.

The ODBP served as the model architecture for the drafting and adoption of the *UOCAVA* Pilot Program Testing Requirements by the EAC.

SUMMARY

The United States is a highly mobile society, and many U.S. citizens live, work, and study abroad. Our Armed Forces, and their dependents, are often called upon to live outside their State of residence, and oftentimes are stationed abroad. The fact that many U.S. citizens and members of our Armed Forces and their dependents are away from their State of residence during federal elections has led to the development of a number of initiatives) to help these citizens exercise their right to vote.

In recent years, FVAP renewed its attention on the use of new information and communication technologies in an effort to help *UOCAVA* citizens register, obtain their ballot information in a timely manner, and return their voted ballots before State deadlines. Because of a longstanding requirement from Congress that FVAP initiate an electronic voting demonstration project, FVAP embarked on an ambitious research agenda to understand the pros and cons of the use of new technologies to solve the ballot transit problem for *UOCAVA* voters and the implications of such technology in a world that possesses more awareness of the need for robust information assurance. At the same time, FVAP continued to engage in services that directly addressed its core mission of ensuring that Service members, their eligible family members, and overseas citizens are aware of their right to vote and have the tools and resources to successfully do so from anywhere in the world.

Section 2 of this report provides further discussion of the statutory context as well as the standards for electronic voting systems for these initiatives. In particular, the context of the congressional requirement for an electronic demonstration project is presented, as is the basic mandate for FVAP. The States have the authority to determine how to run elections in their jurisdictions, and thus FVAP does not have the ability to compel State participation in an electronic voting demonstration project. This context is an important component of the story behind FVAP's research agenda and its ultimate findings.

Section 3 summarizes the research agenda, focusing primarily on the research FVAP conducted as it sought to fulfill the congressional requirement for an electronic voting demonstration project. These studies are part of a continuum that essentially began in 2000 and 2004 with VOI and SERVE, and then were expanded upon later in the decade with research on kiosk-style voting alternatives; other forms of electronic ballot distribution; and basic research into usability, risk assessment, and voting system security. The important research reports that are part of this agenda are discussed and evaluated in this section.

Section 4 presents a strategy for moving forward. The NDAA FY 2015 repealed the congressional requirement for FVAP to conduct an electronic voting demonstration project, but this research remains relevant to States and other election jurisdictions as they seek to find new ways to make the voting process for their *UOCAVA* citizens more usable, accessible, and secure. Thus, in this section, the report concludes by presenting a series of recommendations on how local and State election jurisdictions and the current standards-setting process can unfold in such a way that, should a State determine it wishes to pursue a full Internet voting solution, it can do so in a fashion that takes advantage of the knowledge gleaned from these extensive research efforts. The risk of a State proceeding without a carefully constructed plan to mitigate information security risks and apply stringent standards is the potential of ultimately failing to successfully field a solution, causing the entire *UOCAVA* voter community to suffer a technological setback.

SECTION 2: STATUTORY CONTEXT FOR FVAP'S INTERNET INITIATIVES

Federal elections are administered by State and local officials through a combined framework of federal and State laws. Federal laws provide a framework for federal elections by regulating when elections are held, establishing what the minimum requirements are for who can vote in federal elections (e.g., enfranchisement of women, language minority voters), limiting requirements States can put on voters that would prevent them from voting (e.g., poll taxes), and establishing requirements of when ballots have to be ready to be sent to *UOCAVA* voters. State laws cover issues such as the design and layout of ballots, the voting technology used, the rules regarding the timing of registering to vote, and the timing of when ballots must be returned and, ultimately, the actual conduct and certification of election results.

Since 2000, Congress has enacted several laws intended to facilitate the *UOCAVA* voting process. These laws have proceeded down two tracks. Track 1 includes the *Help America Vote Act (HAVA)* of 2002 and the *Military and Overseas Voter Empowerment (MOVE) Act* of 2009. Both *HAVA* and the *MOVE Act* contain a broad array of provisions that seek to improve the registration and voting experience for *UOCAVA* citizens and provide general research authority to the EAC and FVAP and the authority to conduct various pilot studies. Track 2 comes from specific DoD authorization bills that authorized the conduct of an electronic voting demonstration project to test the feasibility of remote electronic voting for military personnel. Before we consider these two tracks, it is important to understand the legal authority that FVAP has related to facilitating *UOCAVA* voting and how FVAP works with other federal agencies.

FVAP'S RESPONSIBILITIES UNDER *UOCAVA*

UOCAVA requires that the entity which implements the Act – currently FVAP – engage in a set of specified activities, including:[16]

1. Consulting State and local election officials in carrying out this subchapter, and ensure that such officials are aware of the requirements of this Act;
2. Prescribing an official post card form [the FPCA, containing both an absentee voter registration application and an absentee ballot application];
3. Developing a Federal Write-In Absentee Ballot (including a secrecy envelope and mailing envelope for such ballot) for use in general, special, primary, and runoff elections for federal office by *UOCAVA* voters who do not receive their absentee ballot, and implementing an online system whereby *UOCAVA* voters can enter their address (or other relevant information) and receive a list of all federal candidates for whom they are eligible to vote;
4. Prescribing a suggested design for absentee ballot mailing envelopes;
5. Compiling and distributing descriptive material on State absentee registration and voting procedures, and to the extent practicable, facts relating to specific elections, including dates, offices involved, and the text of ballot questions;

[16] FVAP's requirements under *UOCAVA* can be found in "Registration and Voting by Absent Uniformed Services Voters and Overseas Voters in Elections for Federal Office," 52 USC §20310, January 7, 2011. Retrieved from http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title52-chapter203&saved=%7CZ3JhbnVsZWlkOlVTQy1wcmVsaW0tdGl0bGU1Mi1zZWN0aW9uMjAzMTA%3D%7C%7C%7C0%7Cfalse%7Cprelim&edition=prelim

6. Reporting to the President and the Congress, not later than the end of each year after a Presidential election year, on the effectiveness of assistance under this subchapter, including a statistical analysis of Uniformed Services voter participation, a separate statistical analysis of overseas nonmilitary participation, and a description of State-Federal cooperation;
7. Prescribing a standard oath for use with any document under this subchapter affirming that a material misstatement of fact in the completion of such a document may constitute grounds for a conviction for perjury;
8. Establishing procedures for collecting marked absentee ballots of absent overseas Uniformed Services voters in regularly scheduled general elections for federal office, including absentee ballots prepared by States and the Federal Write-In Absentee Ballot, and for delivering such marked absentee ballots to the appropriate election officials;
9. Taking actions as may be necessary (a) to ensure that absent Uniformed Services voters who cast absentee ballots at locations or facilities under the jurisdiction of the Presidential designee are able to do so in a private and independent manner; and (b) to protect the privacy of the contents of absentee ballots cast by absentee Uniformed Services voters and overseas voters while such ballots are in the possession or control of the Presidential designee;
10. Developing online information portals to inform absent Uniformed Services voters regarding voter registration procedures and absentee ballot procedures available for federal elections and establishing a program, using the military global network, to notify absent Uniformed Services voters 90 days, 60 days, and 30 days prior to federal elections, of voter registration information and resources, the availability of the Federal Post Card Application, and the availability of the Federal Write-In Absentee Ballot; and
11. Working with the Election Assistance Commission and the chief State election official of each State, develop standards for States to report data on the combined number of absentee ballots transmitted to absent Uniformed Services voters and overseas voters for the election and the combined number of such ballots which were returned by such voters and cast in the election, and making these data available to the public.

With this context, we can now consider the specific impact of recent congressional actions related to *UOCAVA* voting in general and electronic voting trials specifically.

HAVA AND THE *MOVE ACT*

The *Help America Vote Act* (HAVA) primarily addressed issues related to voter registration and voting technologies in the various States. Several studies found problems associated with *UOCAVA* voting in the 2000 election – including ballots received after the election, ballots without postmarks, ballots postmarked after the election, ballots without witness signatures – and this spurred Congress to include in *HAVA* proposals to improve aspects of the *UOCAVA* voting process.[17] *HAVA* also established the EAC, and most of the requirements related to military voters in *HAVA* were delegated

[17] For media coverage of these studies, see David Barstow and Don Van Natta Jr., "How Bush Took Florida: Mining the Overseas Absentee Vote," *New York Times* July 15, 2001. Retrieved from http://global.nytimes.com/2001/07/15/national/15BALL.html?pagewanted=print&_r=0 Also see Kosuke Imai and Gary King, "Did Illegal Overseas Absentee Ballots Decide the 2000 U.S. Presidential Election?" *Perspectives on Politics*, 2004, 2, pp. 537-549; Diane H. Mazur, "The Bullying of America: A Cautionary Tale About Military Voting and Civil-Military Relations," *Election Law Journal*, 2005, 4(2), pp. 105-131.

to the EAC, not FVAP, but these requirements provide context for FVAP's subsequent work related to remote electronic voting.

In *HAVA*, the EAC was tasked with conducting studies related to ways of improving the registration and voting processes for *UOCAVA* voters. Specifically, in Section 242, "[The EAC], in consultation with the Secretary of Defense, shall conduct a study on the best practices for facilitating voting by absent Uniformed Services voters (as defined in section 107(1) of the *Uniformed and Overseas Citizens Absentee Voting Act*) and overseas voters (as defined in section 107(5) of such Act)."[18] In Section 245, the EAC was also tasked with studying electronic voting, including "the possible methods, such as Internet or other communications technologies, that may be utilized in the electoral process, including the use of those technologies to register voters and enable citizens to vote online, and recommendations concerning statutes and rules to be adopted in order to implement an online or Internet system in the electoral process."[19]

HAVA also called on the National Institute of Standards and Technology (NIST) to provide technical support to the EAC as it developed the Voluntary Voting System Guidelines (VVSG). As noted in Section 221 of *HAVA*, NIST provides technical support in the EAC's deliberation on voting system guidelines and includes issues such as "the security of computers, computer networks, and computer data storage used in voting systems; methods to detect and prevent fraud; the protection of voter privacy; the role of human factors in the design and application of voting systems, including assistive technologies for individuals with disabilities (including blindness) and varying levels of literacy; and remote access voting, including voting through the Internet."[20]

In 2009, Congress passed the *MOVE Act* "to provide greater protections for Service members, their families and other overseas citizens. Among other provisions, the *MOVE Act* requires States to transmit validly-requested absentee ballots to *UOCAVA* voters no later than 45 days before a federal election, when the request has been received by that date, except where the state has been granted an undue hardship waiver approved by the Department of Defense for that election."[21] The *MOVE Act* does not address voting or technology standards related to the electronic transmission of ballots, but it does attempt to address the ballot transit time problem by increasing the time available to vote.

Department of Defense Internet Voting Requirement and its Repeal

FVAP's work related to remote electronic voting has largely been driven by congressional requirements. Congress has included in several NDAAs language requiring DoD to conduct an electronic voting demonstration project.

In 2001, Congress enacted the National Defense Authorization Act (NDAA) for Fiscal Year 2002. Section 1604 of the Act states:

---

[18] Help America Vote Act of 2002, Public Law 107-252. Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-107publ252/html/PLAW-107publ252.htm

[19] Ibid.

[20] Ibid.

[21] U.S. Department of Justice, Office of Public Affairs. "Fact Sheet: MOVE Act." October 27, 2010. Retrieved from http://www.justice.gov/opa/pr/fact-sheet-move-act

> The Secretary of Defense shall carry out a demonstration project under which absent Uniformed Services voters are permitted to cast ballots in the regularly scheduled general election for federal office for November 2002 through an electronic voting system. The project shall be carried out with participation of sufficient numbers of absent Uniformed Services voters so that the results are statistically relevant.[22]

The Act also gives the Secretary of Defense the ability to delay implementation of this demonstration requirement:

> If the Secretary of Defense determines that the implementation of the demonstration project under paragraph (1) with respect to the regularly scheduled general election for federal office for November 2002 may adversely affect the national security of the United States, the Secretary may delay the implementation of such demonstration project until the regularly scheduled general election for federal office for November 2004.[23]

In October 2004, Congress passed the Ronald W. Reagan NDAA for Fiscal Year 2005. Section 567 of the Act was entitled "Repeal of Requirement to Conduct Electronic Voting Demonstration Project for the Federal Election to be held in November 2004." It stated:

> The first sentence of section 1604(a)(2) of the National Defense Authorization Act for Fiscal Year 2002 (Public Law 107–107) is amended by striking ''until the regularly scheduled general election for federal office for November 2004'' and inserting the following: ''until the first regularly scheduled general election for federal office which occurs after the Election Assistance Commission 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.'[24]

In summary, the NDAA FY 2001 required a pilot to be conducted in 2002, and the NDAA FY 2005 provided that a pilot should occur after there are voting guidelines for electronic absentee ballots and after the EAC certifies that it will assist DoD in this effort. The wording associated with the NDAA FY 2005 created a significant limitation for FVAP to consider, because it effectively created a two-year time frame to develop, test, and field an electronic voting demonstration project system.

The EAC established the *UOCAVA Pilot Program Testing Requirements* in 2010. These requirements outline the manner in which the EAC would evaluate a pilot program that could potentially address the DoD electronic voting requirement using a remote kiosk approach, as discussed previously, with a paper record to mitigate security concerns.

In December 2014, section 593 of the NDAA FY 2015, enacted in December 2014, repealed Section 1604 of the NDAA FY 2002 – the original requirement for FVAP to conduct the electronic voting demonstration project.

---

[22] National Defense Authorization Act for Fiscal Year 2002. Public Law 107-107, Section 1604 (2001). Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-107publ107/html/PLAW-107publ107.htm

[23] Ibid.

[24] Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005. Public Law 108-375, Section 567 (2004). Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-108publ375/pdf/PLAW-108publ375.pdf

KEY CONCEPTS FROM NDAA LANGUAGE

Electronic Voting System: "An electronic voting system is one or more integrated devices that utilize an electronic component for one or more of the following functions: ballot presentation, vote capture, vote recording, and tabulation. A Direct Recording Electronic (DRE) voting device is a functionally and physically integrated electronic voting system which provides all four functions electronically in a single device. An optical scan (also known as marksense) system where the voter marks a paper ballot with a marking instrument and then deposits the ballot in a tabulation device is partially electronic in that the paper ballot provides the presentation, vote capture and vote recording functions. An optical scan system employing a ballot marking device adds a second electronic component for ballot presentation and vote capture functions."

Cast Ballot: A cast ballot is a "ballot that has been deposited by the voter in the ballot box or electronically submitted for tabulation."

Statistically Relevant: Typically, social scientists would use the terminology of "statistical significance" or "statistical power" instead of "statistically relevant." When evaluating the effectiveness of a policy intervention intended to address a problem – here, the provision of remote electronic voting – on a target population, researchers need to have enough participants in the study in order to be able to measure the effectiveness of the intervention. A variety of factors have to be taken into account when determining the number of participants needed to be able to measure the effectiveness of the intervention, including the specific outcome or outcomes they wish to assess, the expected size of the potential intervention, the need to measure the outcome effects on subpopulations (e.g., Navy personnel deployed on ships or National Guard troops in forward combat areas) and an understanding of potentially confounding factors. All of these factors have implications on the size of the population needed for an evaluation study.

[U.S. Election Assistance Commission. *Volume I: Voting System Performance Guidelines*, Appendix A: Glossary, A-6, A-10.Retrieved from http://www.nist.gov/itl/vote/upload/VVSG-Volume-IAppendixA.pdf; the definition for "statistically relevant" comes from *UOCAVA*.]

THE ROLE OF THE EAC

Created in 2002 as a part of *HAVA*, the EAC was given several critical tasks related to Internet voting. In conjunction with technical support from NIST, the EAC was to develop voluntary voting system guidelines related to "remote access voting, including voting through the Internet."[25] The EAC was also tasked with conducting a comprehensive study of how Internet technologies could be incorporated into federal, State, and local electoral processes. This study was to include an evaluation of how the Internet could be used to register voters, facilitate voting, and inform voters

[25] Help America Vote Act, H.R. 3295, Section 221, (January 23, 2002). http://www.eac.gov/assets/1/workflow_staging/Page/41.PDF

about the electoral process. These tasks make the EAC an important actor in the ongoing efforts related to studying and implementing a remote electronic voting pilot.

EAC Report to Congress on Remote Electronic Voting

In April 2010, the EAC submitted the *Report to Congress on EAC's Efforts to Establish Guidelines for Remote Electronic Absentee Voting Systems*. The report provided a roadmap describing the EAC's efforts to work with NIST, FVAP, and other organizations to establish these guidelines.

As the report's introduction notes:

> The goal of this project is to develop EAC certified guidelines to aide [sic] FVAP's development of an absentee voting system to serve Uniformed Service voters in a demonstration project administered by the Department of Defense. In addition, the EAC hopes to provide election officials with a resource to improve services for *UOCAVA* voters, with the ultimate goal of improving voter participation rates in this population….
>
> EAC, FVAP and NIST, have made significant progress toward assisting election officials with providing services to *UOCAVA* voters. However, solutions to the challenges that face *UOCAVA* voters will also require a broad community effort with participation from State and local election officials, computer science researchers, experts in fields such as usability and accessibility, industry representatives, and other federal agencies charged with improving the remote *UOCAVA* voting process. To that end, EAC will continue to solicit input from its statutory boards and the public; and work with NIST and FVAP to ensure that the remote electronic absentee voting guidelines are considered and robust.[26]

The report then outlines four milestones and two interim steps in the process of developing guidelines for remote electronic absentee voting:

1. Perform initial research and create initial guidance including establishment of a baseline level of security assurance necessary;
2. Create a current specification for a remote kiosk pilot electronic absentee voting system to analyze the scalability and challenges posed by a multi-jurisdictional kiosk system, and to collect data on the impact of more widespread use of such a system compared to the previously modest pilot programs done in this area;
3. Identify and specify aspects of remote electronic absentee voting that election officials can implement now (e.g., blank ballot distribution); and
4. Implement a phased, iterative approach for remote electronic absentee voting pilots to determine approaches that best meet the needs of *UOCAVA* voters and provide adequate security precautions.[27]

Because significant challenges to remote electronic absentee voting exist, there are also a number of interim actions outlined in this roadmap, including:

---

[26] U.S. Election Assistance Commission. *Report to Congress on EAC's Efforts to Establish Guidelines for Remote Electronic Absentee Voting Systems,* (April 26, 2010) 3. Retrieved from http://www.fvap.gov/uploads/FVAP/Reports/eacroadmap.pdf

[27] Ibid., 5.

1. Facilitate sending blank ballots electronically to improve *UOCAVA* voter participation rates; and
2. Investigate secure platforms for transmitting electronically marked ballots for testing and pilot projects.

The roadmap and work outlined in the EAC report to Congress was effectively halted in 2011 when the EAC lost Commissioners to facilitate the federal advisory committee process to consider and adopt appropriate standards and further a consensus view. On December 16, 2014, three EAC Commissioners were confirmed by the U.S. Senate permitting the renewed operation of its federal advisory committee structure and standards development process. Upon their appointment, the EAC adopted new standards that can be used to test Internet voting systems; however, this development occurred subsequent to FVAP's research. Setting aside these recent developments, FVAP's research and consideration of the demonstration project reflected the environment at the time.

VOTING SYSTEM STANDARDS

As noted in the early FVAP projects examining remote electronic voting systems for *UOCAVA* citizens, such as VOI,[28] there was a pressing need for the development of standards for these new voting systems. From the earliest remote electronic voting projects developed by FVAP, there has been a call for the development of thorough voting systems standards for remote electronic voting systems. For example, one of the key recommendations in the 2001 VOI evaluation report was that FVAP continue to participate in the development of remote Internet registration and voting system standards.

Standards provide benchmarks against which voting systems can be tested and evaluated. Well-designed voting system standards will help ensure that voting systems meet the many desirable attributes of a proper voting system.

The history of the voting systems standards process is complex, and is partly explained by the nature of election administration in the United States. Article 1, Section 4, of the U.S. Constitution generally provides authority over election administration to the States: "The Times, Places and Manner of holding Elections for Senators and Representatives for members of Congress, shall be prescribed in each State by the Legislature thereof; but the Congress may at any time by Law make or alter such Regulations, except as to the Places of chusing Senators."[29] Although the Federal Government can clearly play a role in establishing rules for federal elections, the States are the central actors in regulating and administering elections.

When electronic voting technologies first began to be employed by election officials in the United States four decades ago, problems with their use generated early calls for systematic voting systems standards. An influential report by Roy Saltman in 1975 recommended the development of voting systems standards, but limited the federal role "to closely observe State efforts to adopt more uniform and responsive practices which include concern for the effective use of computing

[28] "While both the DoD and State of Florida standards and procedures [for testing information systems and voting systems, respectively] were comprehensive, neither addressed Internet voting systems." Federal Voting Assistance Program, *Voting Over the Internet Pilot Project Assessment Report*, p. 1-12.

[29] U.S. Const. art. 1 sec. 4. Retrieved from http://constitutioncenter.org/constitution/the-articles/article-i-the-legislative-branch

technology in vote-tallying," and a call for the Federal Government "to foster the establishment of a National Election Systems Standards Laboratory".[30]

Saltman's report led to the development of the first set of *voluntary* voting systems standards by the Federal Election Commission (FEC) in 1990.[31] These early standards were updated by the FEC in 2002, in the wake of the 2000 presidential election and the attention paid after that election to voting technologies and election administration. One of the key aspects of *HAVA* (2002) was the creation of the EAC, and the shifting of responsibility for voting systems standards from the FEC to the EAC. The EAC initiated a process that led to the creation of another set of voting systems standards, which were adopted in 2005. At the time of this research, the 2005 VVSG was the most recent iteration of federal voting systems standards in the United States, as subsequent revisions remain in draft form at the time of this report. Although voluntary in nature, the VVSG and standards adopted by the EAC are the de facto standard used by the majority of States to certify voting systems. Therefore, any successful effort for a mult-state or mult-jurisdictional Internet voting effort would require a system that successfully adheres to conformance testing against applicable standards. The lack of applicable standards at the time this research was initiated and completed remained a key concern for FVAP progress toward meeting the requirement of conducting an electronic voting demonstration project.

FVAP AND ITS ROLE IN ELECTION ADMINISTRATION

The significant role of the States in conducting elections results in limitations and complexities for any centralized electronic voting effort, such as those studied by FVAP in its recent research under the now-repealed electronic voting demonstration project requirement. Essentially, how could FVAP conduct an electronic voting demonstration project at a sufficient scale while meeting the threats of the information security environment without infringing on the authority of the States?

The first problem that arises is that the United States has a highly decentralized structure of election administration. This decentralization has led to an extremely complex patchwork of election rules, regulations, and procedures. Each State has very different laws and regulations regarding the basic conduct of elections. This complexity is one of the important reasons for the existence of the FVAP; to help *UOCAVA* voters navigate the complicated differences in deadlines and election procedures that exist across the States. Although FVAP does provide voters and election officials with information on the voting process for the *UOCAVA* population, the ultimate responsibility for certifying the results of an election rests with each State and its State election official.

The ever-changing threat environment and recognition of information security capabilities within DoD creates pressures for FVAP to expand its role in serving *UOCAVA* voters directly. FVAP has continually

[30] National Bureau of Standards, Institute for Computer Sciences and Technology, Information Technology Division. "Effective Use of Computing Technology in Vote-Tallying," by Roy Saltman. NBSIR 75-687, National Bureau of Standards. (Washington, D.C., 1975), 88-89. Retrieved from http://csrc.nist.gov/publications/nistpubs/NBS_SP_500-30.pdf

[31] The National Institute for Standards and Technology and the EAC have provided histories of the voting system standards process: National Institute for Standards and Technology, "History of the Voting System Standards Program (as of November 1998)," 1998. NIST.gov, retrieved from http://www.nist.gov/itl/vote/upload/wiley.pdf; Election Assistance Commission, "Voluntary Voting System Guidelines Fact Sheet," www.eac.gov, 2015, retrieved from http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines_fact_sheet.aspx

worked to find solutions that serve the needs of *UOCAVA* voters while recognizing that voting activities remain under the control of State and local election officials. This awareness is particularly important as FVAP's core mission is to serve as a source of critical information on the *UOCAVA* voting process, not to be involved in the transmission or receipt of registration or balloting materials.

The depth of these complexities arose during the SERVE project, and has become a recurrent theme in discussions of how FVAP considered conducting an electronic voting demonstration project. For a centralized remote electronic voting demonstration project, there are issues related to how State laws and regulations would affect the development and implementation of such a system. For either type of demonstration, the issues would likely include, but not be limited to:

- Variations across States related to ballot design. States typically have specific laws related to the size of font, order of candidates, having straight party voting options, candidate ordering, ballot designations of candidates, and related matters. This means that the ballot interface for any remote electronic voting system has to be unique for almost every State; and
- Security requirements related to using the Internet in voting. Some States have very strict laws and regulations related to having any voting technology connected to the Internet or related networks. Such regulations can limit the ability of States to participate in a remote electronic voting initiative.

For a remote electronic voting demonstration, there would be variations as well, the most important being:

- Differences across States regarding when absentee ballots must be returned to the local election official. State variations in the deadline for submitting ballots means that the system has to be able to "turn off" for some States, based on the deadline for receiving ballots.

There are even more issues specific to the implementation of a multistate kiosk system. The FVAP report *The Potential for Kiosk Voting in Nine States* found that the issues would likely include:

- Determining which State laws apply to a remote kiosk voting system. Of those States surveyed, many found that a kiosk-based system would likely be considered an early voting/in-person absentee voting location, so in almost all States, laws governing polling places would arise and impact the consideration of such an effort.
- Regulating who can be in a remote kiosk location. Most States do not allow people from outside of their own State to be in a voting location.
- Regulating election observers. Most States have strict legal limits on the number of observers or watchers who can be in a polling location.
- Regulating who can staff a remote kiosk. Almost all (if not all) States require election workers be registered voters in the State or even a registered voter in the local jurisdiction that administers the election. Some States also require partisan balance among election workers that could affect staffing as well.[32]

[32] U.S. Department of Defense, Federal Voting Assistance Program. *The Potential for Kiosk Voting in Nine States*, Alexandria, Virginia: March 2013.

In addition to these logistical concerns, there still remain the concerns about the security and integrity of a remote voting system that led to the cancellation of the SERVE project in 2004. In the intervening years the understanding regarding the potential and realized security threats to any computer network-based system have only become more apparent, and more numerous. Mitigating the security risks inherent in a remote electronic voting system would likely require a higher degree of centralization at the federal level. In the end, such a highly centralized system would imply that the processing and handling of voted ballots would occur in a concentrated and aggregated fashion within the executive branch. This type of system raises the question of whether the passing of election materials, including voted ballots, in this fashion would be changing the role of the Federal Government in the conduct of elections from facilitator to administrator. The lines of accountability associated with continuity and security of a remote electronic voting system, and the proper "owner" of such a system in a wholly electronic voting environment, raise new questions over who is responsible for ensuring the integrity of an election.

Another issue of concern is in regard to the language in the congressional requirement that FVAP ensure that a "statistically relevant" number of military *UOCAVA* voters participate in the demonstration project. Exactly what would constitute a "statistically relevant" participation rate of military *UOCAVA* voters in an electronic voting demonstration project is unclear.[33] Additionally, as the target participation number increases, FVAP would be compelled to seek the involvement of a larger number of States, or to focus the demonstration project on States with large populations of military *UOCAVA* voters. The requirement for a "statistically relevant" number of military *UOCAVA* voters also complicates certain types of electronic demonstration projects, especially remote kiosk voting solutions, because they involve the location of voting terminals in locations with larger numbers of military *UOCAVA* voters from certain counties or States. Unless a large number of States agree to participate in an electronic voting demonstration project (cooperation that FVAP cannot compel), FVAP may not be able to produce an electronic voting demonstration project that is scientifically and statistically meaningful.

SUMMARY

There are three important points made in this section that have significant bearing on FVAP's ability to conduct the electronic voting demonstration project as originally required by Congress.

First, FVAP's mission to provide voting assistance to *UOCAVA* citizens is not necessarily consistent with the development of innovative and complex technological solutions that would be required in a large-scale demonstration project. Although FVAP does have express authority to conduct technology pilot programs, this authority does not require FVAP to develop new voting technologies; in particular, remote electronic voting systems. Rather, Congress required that FVAP "carry out" an electronic voting demonstration project (until that requirement was eliminated in the NDAA FY 2015). With FVAP as an implementer, not developer, and the consideration for a two-year time frame to acquire, test, and field a remote electronic voting system, the use of existing commercial products for the

[33] Typically, scientists will use the terminology of "statistical significance" or "statistical power" in a situation like this. To evaluate the effectiveness of an intervention – here the provision of remote electronic voting – on a target population, researchers will have an outcome or outcomes they wish to assess, an estimate of the (continued from previous page) potential treatment effect, and an understanding of potentially confounding factors. All of these factors have implications for the size of the groups needed for an evaluation study.

conduct of an electronic voting demonstration project became the most viable approach, as well as the consideration of an interim pilot using a remote kiosk architecture.

In addition, since the cancellation of SERVE in January 2004, States have conducted their own electronic voting demonstration or pilot projects. FVAP recognized the value of these pilot efforts in terms of the longer-term contributions to the election community, so it funded a small research effort to evaluate the Okaloosa kiosk-based pilot and worked to identify the barriers that would need to be addressed in facilitating a multistate kiosk pilot.[34] The Okaloosa reports found that even if FVAP were to continue work in this area, it would be the States that would have to harmonize their laws with an electronic pilot demonstration, and the States would have to develop and implement any system.

Second, a critical hurdle that will need to be met for the development and deployment of new remote electronic voting systems for *UOCAVA* voters are standards for those systems, as well as a certification and testing process. This was FVAP's operating assumption after Congress passed the NDAA FY 2005, which signaled that FVAP should wait for the applicable standards before proceeding. Since then, the EAC adopted Version 1.1 of the VVSG which does provide the ability for *UOCAVA* system testing; however, the absence of standards at the time did represent a significant challenge for FVAP's effort.

The role of State governments in election administration creates a vast amount of complexity that will make the development of a multistate electronic voting system difficult, complicated, and expensive. As any electronic voting demonstration project is scaled upward to the meet the "statistically relevant" threshold, this level of complexity would only increase and jeopardize FVAP's ability for success because it has no authority to force States to participate in an electronic voting demonstration project.

These observations stand in sharp contrast to the need to develop a highly secure and robust electronic voting architecture that could rely, in key places, on current U.S. Government information technology infrastructure. For example, FVAP studied the use of the CAC architecture so that *UOCAVA* citizens in possession of a CAC could use it to access the secure U.S. Government Non-classified Internet Protocol Router Network (NIPRNet). Although this could provide a secure and robust means for citizens to access their balloting materials electronically, it also means that U.S. Government network infrastructure would be used for some aspects of the collection and transmission of ballot materials. At a minimum, this is an important point of reference not only in terms of this specific requirement for the electronic voting demonstration project in hindsight, but also in terms of the importance of identifying the interplay between technology and election policy for the election community moving forward and who is the responsible party for upholding the integrity of an election.

This context is critically important for understanding and considering FVAP's research agenda to meet the electronic voting demonstration project requirement. In Section 3 of this report, that research agenda is presented and analyzed in detail.

---

[34] See the reports *The 2008 Okaloosa Distance Balloting Pilot Project* and *The Potential for Kiosk Voting in Nine States* for a discussion of the Okaloosa pilot and the barriers to expanding this pilot to other jurisdictions and States.

SECTION 3: FVAP'S RESEARCH ON REMOTE ELECTRONIC VOTING

In its *Report to Congress on EAC's Efforts to Establish Guidelines for Remote Electronic Absentee Voting Systems* from 2010, the EAC provided a roadmap that would leverage FVAP's pilot program authority to conduct remote kiosk-based pilot initiatives provided under the *MOVE Act*. A key aspect of this roadmap was conducting supporting research for the eventual development of voting system standards (VSS) for an entirely electronic voting demonstration project that would allow FVAP to meet its original NDAA FY 2002 requirement. In August 2010, the EAC, NIST, and FVAP conducted a joint meeting to engage key stakeholders directly on the outstanding issues surrounding the consideration and adoption of VSS for an entirely remote electronic voting absentee voting system. FVAP embarked on an approach that simultaneously intended to satisfy its original requirement and also tried to assist with a standards development process.

During this joint meeting in 2010, various topics were framed for discussion to spur development of the relevant standards and to honor the original timeline specified in the EAC's *Report to Congress*. These topics included authentication, privacy, auditability, network security, and the security of the systems that would host the voting applications and information. These topics were identified as key aspects for understanding the acceptable level of risk for the current *UOCAVA* mail-based voting process ballots compared with that of a remote electronic voting system. Rather than employing a remote kiosk model in this approach, the understood environment was to be an unsupervised remote electronic voting environment.

FVAP held three research summits in 2010 and 2011, where the discussion topics noted previously were discussed in breakout groups consisting of various stakeholders in the process – including computer scientists, government officials, and election officials – to identify outstanding questions that would enable comparisons between the current paper-based voting process and a remote electronic voting process. The following summits were held:

- August 6-7, 2010: "Workshop on *UOCAVA* Remote Voting Systems," Washington, DC;
- March 23-24, 2011: "*UOCAVA* Solutions Working Group," Chicago, IL; and
- August 6-7, 2011: "*UOCAVA* Solutions Working Group," San Francisco, CA.

Below are key research questions posed to each breakout group that served as the initial framework for FVAP research agenda:

- What type of FVAP-sponsored conformance test should be used to accredit these systems against the *UOCAVA* Pilot Program Testing Requirements (UPPTR)?
  - What is the impact of this conformance test against the timeline for implementing a remote kiosk-based approach?
- What is the level of resistance existing systems possessed against penetrations?
  - What is the eventual type of approach and methodology FVAP should consider for a large-scale implementation of a penetration test as part of its security posture?
- What are the relative benefits/concerns with using the Defense Information Systems Network (DISN) as part of the overall architecture?
  - Could the Department consider the use of a standardized client configuration as part of its remote electronic voting system?

    - What would be the supporting logistics associated with this?
- What is the role of the Department's Common Access Card (CAC) for system authentication purposes?
    - What is the potential for its use as part of the voter authentication process?
- What is the supporting statutory and legal framework for the States to participate in a remote kiosk-based pilot?
- What is the comparative level of risk between the existing postal-based system and that of a remote electronic voting system and can this risk be quantified?
- Would the advent of software assurance tools hold value for identifying the extent of known defects in software source code?
    - Could these tools be used to assist with source code reviews? What is the extent of coverage that software assurance tools could provide?

CHARTING A PATH FOR COMPLIANCE

The complexity of fulfilling the requirement of the electronic voting demonstration project, as outlined in the NDAA FY 2002, or conducting various pilot initiatives under the *UOCAVA* Pilot Program Testing Requirements (UPPTR), eventually led to the development of a two-track system for its research– a remote kiosk-based voting system and a remote electronic voting system – for FVAP to consider as part of its future planning efforts. FVAP's efforts to meet its congressional mandate were affected by the absence of a quorum of EAC Commissioners between December 2011 and January 2015. This forced FVAP to reconsider its approach to the original congressional requirement for a demonstration project, absent directly applicable standards. The research studies discussed in this section were intended to evaluate both of these approaches as FVAP considered how to move forward.

The original requirement to conduct the electronic voting demonstration project was amended in 2005 to provide discretionary authority to FVAP to wait for voluntary voting system standards for remote electronic voting to be issued by the EAC. However, once these standards were issued, FVAP was required to conduct an electronic voting demonstration project in the next general election. At best, this granted FVAP a two-year window to:

- Navigate the acquisition process;
- Develop a system;
- Integrate such a system, if necessary, into the DoD network;
- Obtain certification that the system met federal security standards;
- Test that the system conformed to the EAC standards, and
- Field the system.

The reality of navigating these lengthy processes led to FVAP's consideration of commercially available remote electronic voting solutions rather than one developed within the Department. As FVAP continued to move forward in its approach, a number of assumptions were taken into account:

1. Commercially available remote electronic voting systems would have to be leveraged;
2. FVAP would have to sponsor a conformance test to the EAC-adopted standards;
3. Only a few States would have the legislative authority in place to support this timetable and provide an opportunity for a statistically relevant rate of participation;
4. A remote kiosk-based pilot could provide valuable research, but may not be feasible or satisfy the original intent of electronic voting demonstration project requirement; and

5. The administrative and legal complexities surrounding election administration would have to be considered in a single approach.

In 2010, FVAP approached this complicated requirement with the understanding that only through a series of engagements with key stakeholders would it be able to develop a consensus-based approach for how this remote electronic voting system would look, how it would perform, and what security posture it would maintain.

CHALLENGES IDENTIFIED DURING THE *UOCAVA* VOTING SUMMIT PROCESS

The *UOCAVA* voting summit process identified a number of important challenges that FVAP would need to address in order to conduct an electronic voting demonstration project. Central challenges were:

- **The contentiousness of remote Internet voting**. This issue is contentious and complex, in particular for computer scientists and cyber-security experts. Because of this, mechanisms would need to be developed in the summit process to facilitate productive and informative conversations. The contentiousness of this issue also clarified the general need for quality research to be conducted on some of the areas of greatest disagreement.
- **The need for comparative risk assessment and evaluation**. One of the most pressing areas of disagreement involved the comparison of risks between potential remote electronic voting systems for the *UOCAVA* population, and the existing means by which *UOCAVA* voters obtain and return their ballots. Developing a research agenda that could identify the risks, determine the relative likelihood of each risk occurring, and quantify those risks was identified as an important issue. The importance of quantifying these risks is a means in which trade-offs can be recognized in any system development.
- **The need for standards and testing**. Another challenge arising from the summit discussions was the lack of existing standards tailored for remote electronic voting systems. The existing EAC VVSG do not contain guidance for the types of remote electronic voting systems typically envisioned for *UOCAVA* voting (neither remote Internet voting nor remote kiosk voting). And, in order for any electronic voting demonstration project to proceed, standards would be important so that systems could be designed to meet and be tested against those standards. During the time the summits occurred, the EAC released its UOCAVA Pilot Program Testing Requirements (UPPTR). The UPPTR was intended to provide standards and best practices that could be used for testing voting systems for use in pilot projects that might occur under *MOVE Act* authorization.
- **Risk mitigation**. Development of a means to mitigate or eliminate the risks associated with a remote electronic voting system for *UOCAVA* voters was also identified as an important research question. Mechanisms for testing and verifying the software used in these systems – and for hardening the security associated with authentication, ballot transmission, and system security – were also identified in the summit process as research priorities.
- **Authentication and security**. The use of CAC technology as an existing architecture for identity authentication, and the NIPRNet to help minimize the presence of malware within a controlled network, was recognized as a particular area needing further research.

The *UOCAVA* voting summit process was successful in that it produced an open dialogue between FVAP and key stakeholders about the electronic voting demonstration project. These summits also helped FVAP reconsider and broaden its research agenda in order to resolve outstanding questions

and security concerns. The key themes that emerged from the *UOCAVA* voting summit process focused on the development of a framework for understanding the key properties of a remote electronic voting system, understanding the key parameters for producing a comparative risk analysis, examining the risks of current *UOCAVA* voting procedures relative to remote electronic voting options, and understanding the overall concerns about the risks of remote Internet and remote kiosk voting systems.

FVAP's resulting research agenda included a series of studies that examined approaches to testing potential electronic demonstration project or pilot program voting systems against the 2010 EAC UPPTR standards, especially the security and usability standards of UPPTR in lieu of more applicable standards. Additionally, FVAP studied the usability and security of the CAC to determine if it could provide greater assurance that potential remote voters are in fact who they claim they are, and also provide potential remote voter access to the NIPRNet system. Another set of research studies focused especially on the remote kiosk voting model for remote voting, based on comments received during the summit process. Finally, FVAP also produced studies examining the development of a prototype process for evaluating the comparative risks of electronic voting against the current by-mail absentee *UOCAVA* voting process, as well as examining whether off-the-shelf commercial software tools are useful for studying electronic voting system source code for known problems and failures to meet coding best practices.

These research studies commissioned by FVAP are reviewed in the rest of this section. The reviews provide a summary of the context of the research, as well as its objectives, accomplishments, and limitations. The goal of these studies was to help FVAP assess the potential for conducting a remote electronic voting demonstration project or pilot project and, taken as a whole, provide a clear picture of both the barriers and possibilities associated with such projects.

TESTING UPPTR

EAC released *UOCAVA Pilot Program Testing Requirements* (UPPTR) on March 24, 2010. Although voting system standards for traditional polling place voting systems have been developed and used by the States, those standards are deficient for remote Internet voting and remote kiosk voting systems. This has been noted in the various remote electronic voting projects conducted in the past. For example, the VOI project discussed earlier in this report used both the existing State of Florida voting system certification process as well as a DoD certification process.[35] The remote kiosk voting project conducted by Okaloosa County, Florida, in 2008 (more details to follow) used Florida's testing and certification process.[36] The lack of comprehensive standards for remote electronic voting systems at the time this research was completed was an important discussion point in the *UOCAVA* voting summits.

The UPPTR provided standards for the testing of *UOCAVA* electronic voting systems, including requirements for system functions, usability, software, quality assurance, configuration management, elements of a technical data package, and the system user's manual. However, the UPPTR left out a complete resolution on the issue of security surrounding a voted ballot transaction

[35] See Section 1.6.4, "Pilot System Testing and Accreditation," in the *Voting Over the Internet Pilot Project Assessment Report*.

[36] See pages 31-34, "System Certification and Approval," in *The 2008 Okaloosa Distance Balloting Pilot Project* report.

and relevant standards. Instead the UPPTR was premised on a kiosk approach to a pilot system, one that provides a paper record of each ballot cast as an interim measure. In order to determine how the UPPTR might be used in an electronic voting demonstration or pilot project, FVAP set out to develop prototype approaches for testing potential remote electronic voting systems against the UPPTR knowing its ultimate approach was to field a wholly electronic voting system—one without a paper record.

This research agenda had three components.

- One component was usability testing, which is in Section 3 of UPPTR. The usability testing approach that was developed and tested is discussed in *Operation VOTE* (September 16, 2011). Because *Operation VOTE* has already been released to the public, it will only be briefly summarized here.
- A second component was a research project that FVAP developed to examine how voting systems testing laboratories might be able to test potential remote electronic voting systems that could be used in a pilot project with respect to Sections 2 (functional requirements) and 5 (security) of UPPTR. *The Voting System Testing Laboratory* (VSTL) *Functionality and Security Testing* report has also been released and is only briefly summarized here.
- The third component of FVAP research aimed at developing processes to determine how they might test potential remote electronic voting systems relative to the UPPTR requirements regarded a specific set of security tests, focused on system penetration, attack detection, and intrusion recovery. The *Penetration Testing of a Simulated Election* report has also been released and is summarized briefly here.

USABILITY TESTING: OPERATION VOTE

Section 3 of the UPPTR focused on usability and the level of usability that is expected from any voting system. *Operation VOTE* focused on the usability, accessibility, and privacy of electronic voting systems. This study, conducted in association with the EAC and DoD's Office of Wounded Warrior Care and Transition Policy, developed and implemented a framework for the evaluation of the general usability of voting systems similar to those that might be deployed in an eventual electronic voting demonstration project.

The study used six off-the-shelf electronic voting systems; three were remote Internet Voting Systems (IVSs), and three were Electronic Ballot Delivery Systems (EBDSs) that were highlighted for use during FVAP's 2010 Electronic Voting Support Wizard (EVSW) project. The usability testing protocol utilized 127 subjects stationed at Brooke Army Medical Center in San Antonio, TX. The subjects comprised 100 Wounded Warriors and 27 Warrior in Transition Unit staff. The Wounded Warrior subjects had a variety of physical, emotional, and cognitive impairments; the staff subjects were included "to ensure the broadest possible testing of system accessibility features."[37]

Each subject was assigned a voting system on which to cast a ballot in a mock election; their use of the voting system was observed, and each observer completed an informational form.[38] Each

[37] U.S. Department of Defense, Federal Voting Assistance Program, *Operation VOTE*, (Alexandria, Virginia, 2011), 16.

[38] See Appendices D and B of *Operation VOTE*, respectively.

subject was then interviewed with a post-use survey.[39] The usability, accessibility, and privacy testing found a number of specific ways in which the electronic voting systems being tested could be improved. Specifically, *Operation VOTE* found a number of ways to improve Section 3 of UPPTR, clarify the requirements, and to make the testing process more efficient. The report recognized some limitations of the research effort, and ways in which future usability testing for Section 3 of UPPTR could be improved through the use of a more realistic testing environment, better training of observers, and improved testing protocol.

Operation VOTE provides a useful foundation for the evaluation of these six voting systems (as they existed in 2011 versions), and for the relative usability and accessibility merits of the IVS and EBDS systems overall. More important, it provides a useful methodology for evaluating the usability, accessibility, and privacy for other *UOCAVA*-oriented electronic voting demonstration projects in the future.

Developing a Process For System Testing: The VSTL Report

The *Voting System Testing Laboratory Functionality and Security Testing* (VSTL) research project sought to develop a process for testing remote electronic voting systems with respect to Section 2 – functionality requirements (e.g., voting capabilities and accuracy) – and Section 5 – security (e.g., communications safety, cryptography, and logging) – of the UPPTR. These issues were identified in the *UOCAVA* voting summits and in previous remote electronic voting trials as being among the most critical. To that end, five Electronic Ballot Delivery Systems (EBDSs) and two remote Internet Voting Systems (IVSs) were selected for evaluation in this research project. Two EAC-accredited voting system testing laboratories conducted the testing (the electronic ballot delivery systems were tested with respect to UPPTR Section 5; the two remote electronic voting systems were tested against Sections 2 and 5 of UPPTR). Given the novelty of the UPPTR, the fact that none of these voting systems had previously been tested with respect to requirements like those contained in the UPPTR, and that the voting system testing laboratories were not as familiar with testing remote electronic voting systems as they were with testing traditional in-person voting systems, this research project had ambitious objectives. In particular, this research initiative sought to determine if testing procedures could be developed and deployed so that these novel voting systems could be adequately tested against the new UPPTR standards. Doing so required a determination as to the adequacy of the UPPTR for testing and, in particular, whether the language in UPPTR was sufficiently accurate and detailed for actual system testing.

As this research report has been previously released, it will only be briefly summarized here. The ambitious objectives of the VSTL research were met; the two voting system laboratories were able to test both types of remote electronic voting systems with respect to Sections 2 and 5 of the UPPTR. In doing the tests, there were several areas where the research effort identified issues with the UPPTR that can be addressed through simple changes to it.

- The UPPTR contains ambiguous language, and this led each testing laboratory to interpret the UPPTR in its own way, leading to differences in testing and test results. Before any further process can be made developing a system for testing remote electronic voting systems against requirements like those in the UPPTR, the requirements themselves need to

[39] See Appendix C of *Operation VOTE*.

be refined to make them more amenable for actual use in a voting system testing environment.

- The voting system laboratories used different testing methodologies, and reported the results of the testing in different ways. Given the novelty of these voting systems, and the UPPTR, this is not a surprise. Standardization of testing methodologies and reporting requirements for voting systems laboratories will insure that testing results are replicable and repeatable.
- The research process only sought to test the remote electronic voting systems with respect to Sections 2 and 5 of UPPTR. None of the other sections of UPPTR were evaluated; these voting systems were not tested against the other sections. Developing methodologies for testing to the other sections of UPPTR, or to future standards such as UPPTR, is a necessary next step.

In reading this report, it is important to remember that the vendors did not, nor were they asked to, provide source code or technical data packages, which in turn meant that neither could be tested. As a result, the findings in this research differ from how they would look in a full-scale testing report. For example, it is typically the case that when problems are found in a testing situation like this, the vendors are allowed to resolve or remediate any problems and submit the voting systems for retesting. In this case, voting systems were tested only once, and vendors did not have an opportunity to either resolve or remediate observed problems because voting system certification was not an outcome of this research. It is possible that if the full certification protocol was followed as outlined in the EAC certification program requirements, those ambiguities identified would likely be resolved through a structured test plan and the Request for Interpretation process.

Developing a Process for System Penetration and Intrusion Testing

The FVAP research agenda also examined the use of penetration testing as part of a security conformance test and as part of a direct offset to the existing UPPTR. The three key objectives of the penetration testing research effort were to (1) determine the level of resistance existing systems possessed against penetrators, (2) develop a proof-of-concept test to examine how penetration testing might be utilized to test the security of remote electronic voting systems, and (3) determine how penetration testing might be incorporated into the potential testing of voting systems for an electronic voting demonstration prior to fielding a live system.

Penetration testing is used to test computer systems against potential attacks from malicious outside entities. In other words, a computer system that is up and running will be subjected to an unknown array of attacks by a team or teams of testers, and the defects identified during the penetration testing can then be remediated or mitigated by vendors. The process can then be repeated as new attacks or new defects emerge.

The proof-of-concept research test that FVAP undertook involved having two different teams of penetration testers examine the three remote electronic voting systems that were registered with the EAC at the time of the testing with two different teams of penetration testers. One team was from *RedPhone/Calibre*, a commercial information security firm, the other team comprised students from the Air Force Institute of Technology. Testing was conducted over a 72-hour period; at the conclusion of the penetration testing exercise, neither team successfully compromised any of the three voting systems being tested. The testing teams did, however, produce a series of recommendations on how the security of these three voting systems could be improved.

The report *Penetration Testing of a Simulated Election* has been previously released, so it will only be briefly summarized here. The penetration testing research met its objective, which was to develop a proof-of-concept project to demonstrate that penetration testing could be used to test the security of remote electronic voting systems, recommendations for improving applicable voting system standards, and it provided a sense of its future scale and implementation prior to fielding a live system. The research suggests several recommendations on how additional penetration testing should be conducted in the future.

- The penetration tests should provide for all types of potential attacks, such as distributed denial-of-service attacks. Also, the testing period should be similar to the period that will be used in an election and replicate industry best practices.
- Similar to the VSTL testing, the penetration testing proof-of-concept study found many areas where section 5 of UPPTR was ambiguous or needed clarification. The lack of clarity with respect to the requirements being tested meant that there was too much leeway for the testing teams.
- And again, as with the VSTL testing, in future testing, vendors should have the opportunity to participate in a mitigation or remediation step in order to determine whether the issues identified by the penetration teams can easily be rectified.

In reading this report, it is important to remember that this was a proof-of-concept study, so the results of the penetration testing are not definitive. Although neither team was able to successfully compromise any of the three systems tested, this does not mean that these systems were fully tested against all possible types of malicious attacks.

Common Access Card (CAC/ Defense Information Systems Network (DISN) Research

Authentication and security were both critical issues that were discussed at the *UOCAVA* voting summit events. One important idea that arose at the summits was for FVAP to determine whether more secure solutions could be leveraged and integrated within the DoD infrastructure. These solutions could provide more secure methods that potential voters might use to access balloting materials or voting applications in a remote electronic voting demonstration or pilot project – an improvement over the potential defects associated with the use of insecure public networks or Internet access points (e.g., public Wi-Fi networks).

To this end, FVAP studied the feasibility of using one of the Defense Information Systems Agency (DISA) networks, NIPRNet, in a potential remote electronic voting demonstration or pilot project. This was studied, along with the feasibility of using the DoD CAC for identification and authorization to access and utilize the NIPRNet. The NIPRNet is a private and secure information transmission network that allows DoD personnel with access to the network to transmit unclassified but still sensitive information to others on the network and to access the broader Internet.[40] It is an example of a "hardened" private network, which uses rigorous access and hardware protocols to assure that it has a higher level of security than is commonly available on public networks. Details of the NIPRNet are available in the CAC/DISN report. The goal of the CAC/DISN research was to determine

[40] A description of the NIPRNet can be viewed at U.S. Department of Defense, Defense Information Systems Agency, The IT Combat Support Agency, "Sensitive but Unclassified IP Data," (2015), retrieved from http://www.disa.mil/Network-Services/Data/SBU-IP

the benefits, and concerns, associated with using the DISN as part of the overall architecture of a remote electronic voting demonstration project; whether DoD could consider the use of a standardized client configuration as part of its remote electronic voting system; and the supporting logistics associated with these uses of DoD infrastructure. This research also considered whether the CAC system had potential as a voter authentication tool in a demonstration project.

The DoD uses a Public Key Infrastructure (PKI) for identification and authentication necessary to access the NIPRNet. The DoD PKI also provides encryption and digital signatures for applications that use the NIPRNet. The DoD CAC provides a holder with the digital identification necessary to access and use the NIPRNet, and it also provides the necessary digital information so that a holder of a CAC can encrypt and digitally sign materials. A CAC physically looks much like a standard credit card, though it contains the electronic circuitry necessary to make it into a "smart card." A holder of a CAC, who also possesses the necessary other factors to use it (typically PIN or biometric information), can access the NIPRNet (as well as other DoD infrastructure that the CAC enables one to access). CACs are issued to DoD personnel and others who need access to DoD infrastructure requiring CAC authentication; they are issued after the identity of the potential holder has been confirmed using a robust and highly structured certificate authority process.

For the purposes of the feasibility study, it was assumed that individuals who might be attempting to access ballot materials or a remote electronic voting application would possess a CAC, would know how to use it to access the NIPRNet, and would have a workstation that they can use with their CAC to access the NIPRNet. This research project then considered a number of potential system architectures whereby potential voters could use a CAC to access the secure NIPRNet, and then (1) access a State or local election official's system in order to confirm their voter registration in that jurisdiction, and (2) either obtain their ballot electronically or interact with a remote electronic voting application.

As a feasibility study, this research demonstrated the steps that would be necessary to integrate the CAC/DISN with a voting system controlled by a State or local election official. This integration would allow potential *UOCAVA* voters to obtain electronic ballot materials or interact with a remote electronic voting application with a higher degree of assurance that their network connection to the election official is not likely to have been compromised.

Should additional research be conducted regarding the CAC/DISN, this report has identified several areas that warrant close consideration.

- CAC is a PKI architecture that is used by DoD and DoD-affiliated personnel. Any remote voting system that assumes CAC/DISN use needs to consider that the population of potential *UOCAVA* voters would be restricted to those with CAC access. That would likely rule out participation of non-DoD *UOCAVA* voters – in particular, U.S. civilians working, living, or traveling overseas – in an electronic voting demonstration or pilot project that uses the CAC/DISN. The alternative would be to develop a process for *UOCAVA* citizens without CAC access to obtain CAC access or digital credentials needed to use a private network akin to the NIPRNet.
- The exact means by which election officials would connect their remote electronic voting systems to the NIPRNet environment remains in question. Election officials could maintain their own remote electronic voting systems and connect in some way to the NIPRNet to provide a secure private network, but this introduces risks because the election officials' systems are located outside the secure NIPRNet infrastructure and therefore are at a

heightened risk for attack and being compromised. On the other hand, the voting systems could be located within the NIPRNet environment, providing more security for those systems. However, this is logistically complicated, given that a multiplicity of election official systems might need to be located in the NIPRNet environment. There would be considerable implications for voting system testing and certification of systems located within the NIPRNet environment as well as the issue of establishing the direct lines of accountability for such a system and maintaining compliance to existing DoD regulations.

- Consideration should be given to the potential risks to FVAP and DoD for allowing CAC and NIPRNet infrastructure to be used for ballot transmission or the casting of electronic ballots. As discussed earlier, the U.S. Constitution gives the authority to conduct elections largely to the States; however, using CAC and NIPRNet would require the transmission of ballot materials through a secure, private, federal network infrastructure. This could be seen as the Federal government, in particular the DoD, being directly involved in the conduct of elections. For example, if the CAC and NIPRNet were used for transmission of voting materials, and questions raised about fraud or tampering using the DISN environment, it could expose DoD, FVAP and voter confidence to significant risk unless clear lines of accountability are established up front.
- Finally, this feasibility study discussed the use of the CAC for authenticating a holder for access to the NIPRNet; however, the use of the CAC for purposes of determining voter eligibility remains an area for further clarification. Future research should consider the possibility that voters, election officials, or the public could misunderstand this process on how the CAC is being used for purposes of granting access to a network versus determining voter eligibility. The CAC would authenticate the holder to access the NIPRNet; however, the CAC would not be used to automatically authorize the holder as an eligible voter in a particular jurisdiction. Election transactions for *UOCAVA* voters rely upon the direct affirmation of their qualifications and this current process should be consistent for all voters.

TESTING SOFTWARE ASSURANCE TOOLS

As a part of its overall effort to develop conformance testing tools – tools to ensure that voting system software meets a defined set of standards for performance – FVAP worked to develop a methodology that could be used to test the quality of source code for a potential electronic voting demonstration or pilot project. Since FVAP was under a mandate to field an electronic voting demonstration project within a two-year time frame (at most), existing commercial products tailored for remote electronic voting were considered the most appropriate for study use. This research process is discussed in the reports *Investigation of the use of Software Assurance Tools on Internet Voting Software Applications*. Software assurance analyses help demonstrate that source code is free of known defects and that the source code operates as designed.[41] The primary objectives of this research effort were to develop a potential approach for the use of commercial and open source software assurance tools to assess the quality of voting system source code, and to improve source code review processes for what would be an entirely software-driven voting system. This is especially important should an unknown defect become identified and a resulting patch needs to rapidly deployed.

[41] For additional discussion of software assurance, see the U.S. National Institute of Standards and Technology, Software and Systems Division, "Software Assurance Metrics and Tool Evaluation (SAMATE) project," (2014), retrieved from http://samate.nist.gov/Main_Page.html

The prototype method developed and tested as part of this research involved the use of an array of software assurance tools to determine whether the use of multiple tools increased the likelihood that actual defects or code defects were identified and the extent of coverage these tools provide for identifying known defects. The research also intended to determine if, as part of this process, it might be possible to make this approach more efficient by filtering out false positives.

The supporting rationale for the development of this approach to software assurance testing for potential electronic voting system software is based on a previous study conducted by the National Security Agency (NSA).[42] That research found, based on known code defects intentionally placed into source code, that the use of multiple software assurance tools, rather than the use of a single tool, increased the likelihood that known code defects would be found in static system testing.

FVAP research focused on three remote electronic voting system vendors – whose remote electronic voting systems were registered with the EAC at the time of this research – with the express purpose of offering an Internet-based voting experience. Of the 23 software assurance tools identified and used in this research, the research team selected specific ones best suited for testing the particular voting system source code.

In this research, the process developed and testing involved a number of steps:

- The research team would use each software assurance tool to examine each voting system vendor's source code.
- The results from that analysis, in particular the defects or coding errors that were identified, were then provided to the voting system vendor. The vendor was asked to confirm or dispute each identified issue.
- The vendor evaluations were then examined by the research team, and they analyzed the vendor's results. At that point, the research team would confirm whether a problem or defect had been correctly identified or not. This process thus differentiated actual software defects ("true positives") from results that the software assurance tools identified as defects that in fact were not defects ("false positives").
- A third-party test laboratory then independently confirmed the research team's analysis and conclusions.

This research demonstrated that a software assurance approach similar to the one developed by the research team could be used expand the identification of known defects and in remote electronic voting software. In that sense, this project successfully demonstrated that software assurance testing procedures could be used to improve the source code in any remote electronic voting source code over time that might be used in a potential electronic voting demonstration project or pilot test. Such an approach could identify and resolve defects and coding defects, and FVAP could then have increased confidence in the security and integrity of the voting system's source code. This is an important consideration for any voting system that is entirely software driven which may rely upon an ability to rapidly deploy security patches in response to an ever-changing threat environment. The use of these software assurance tools throughout the software

[42] For example, see the report by U.S. National Security Agency, Center for Assured Software, *CAS Static Analysis Tool Study – Methodology,* 2011, retrieved from http://samate.nist.gov/docs/CAS_2011_SA_Tool_Method.pdf

development lifecycle would provide dividends in the ability of any entity to establish a proper baseline for the software under review and deploy software upgrades in a more efficient manner.

Although this research effort demonstrated the potential utility of the use of multiple software assurance tools for testing remote electronic voting system source code, there are several points that deserve further investigation.

- All true positives detected were validated with the manufacturer to demonstrate the effectiveness of the tools.
- The software assurance reports found that the approach developed here is potentially costly and time-consuming; however, conducting a line-by-line source code review process can be just as costly and time consuming. Using this software assurance testing process could be difficult to implement if a potential pilot project had a short lead time to implementation. However, continued usage of these tools over time could lead to overall cost efficiencies.
- The prototype developed here could be deployed in a number of different ways. For example, it could be used in the testing and certification process; standards could assert what sort of results from software assurance testing could result in certification and use for an electronic voting demonstration or pilot project. This process could also be used in the selection of commercial voting systems for a *UOCAVA* remote electronic voting project; systems that met certain thresholds could be selected for further evaluation before use. Software assurance testing and usage holds the most value when it is used during source code development as part of the overall software development life cycle.
- The ultimate efficacy of these tools needs further review because the supporting initial research examined a source code that already reflected a scoring of known defects. This points to the inherent value for conducting an initial line-by-line review of source code to establish a baselines. In this research exercise, the commercial software did not have this initial diagnostic available – so further research is required in this area to truly isolate the confidence level that can be attributed to the continued use of these software assurance tools. However, this research exercise marks an important first step.

Manual source code review is obviously difficult, time-consuming, and may or may not detect defects. Automated software testing, similar to that discussed in these reports, is also susceptible to these same criticisms. Whether automated software testing is superior to manual software testing, in the context of remote electronic voting system software, requires further study. In particular, both the costs of each approach and the rate at which each identifies potential problems in source code need further study. The most prudent approach would use the tools as part of an overall approach—not a panacea.

REMOTE KIOSK VOTING RESEARCH

Many critiques of remote Internet voting have noted that some of the security concerns can be mitigated by having the voting done at remote Internet kiosks under the control of election officials. This allows the election officials to ensure that the voting equipment is secure, that voters are authenticated in the same way as voters at a polling place, and allows for the voting process to be audited, especially if there is a paper ballot record produced during the voting process. The goal of remote kiosk voting research was to determine how kiosk voting has worked in practice and whether States have supporting statutory and legal frameworks that would support participating in a remote kiosk voting pilot project. FVAP considered the viability of a kiosk approach to meet the requirement

for the conduct of an electronic voting demonstration project and attempt to leverage the existing UPPTR to meet compliance.

OKALOOSA DISTANCE BALLOTING PROJECT

In 2008, Okaloosa County, Florida, conducted a remote kiosk Internet voting pilot. This project is generally viewed as being a successful, albeit limited, demonstration of remote kiosk voting. The implementation of the pilot is discussed in detail in the report *The 2008 Okaloosa Distance Balloting Pilot Project (*December 2012, hereafter referenced as ODBP*)*. The report explains its implementation and provides information regarding the users of the system. The ODBP notes:

> The kiosk system was implemented in three locations: Germany, Japan, and the United Kingdom, proximate to U.S. military installations in Mildenhall, England; Ramstein, Germany; and Kadena, Japan. The kiosks themselves were not located on military bases so as to not limit access to only military voters, and all qualified military and civilian voters in the vicinity who submitted a request to vote by this method could use the kiosks. The sites were open from October 24, 2008, through November 2, 2008, (with some variation for individual site issues) and were staffed by experienced Okaloosa County poll workers who traveled to the locations for this work (page 1).[43]

In regard to who used the system:

> Ninety-three voters ultimately used the system [and 91 completed a survey of their experience]. These [survey] data indicated that all respondents found the system easy to use and indicated they would vote using an Internet kiosk again. The typical user of the system traveled for 10 minutes or less to get to the kiosk location. However, when asked how far they would be willing to travel to vote on a kiosk system, the average respondent said they would travel 30 minutes or less. Remote kiosk voters were more likely to be male, college graduates, and military personnel (page 2).[44]

The report's primary value comes from an analysis of the key issues that arose during its implementation. These issues can be divided into three categories: legal, procedural, and logistical. The report identified two primary legal issues. First, for any similar voting project to be successful, the State must have a legal structure that allows for remote kiosk Internet voting. Having a State law that allows for experimentation is critical in facilitating programs like Okaloosa's. Second, as each State has a different process and requirements, any future multistate kiosk voting project will need to have a well-structured plan for testing and certification in place long before planned implementation.

The ODBP identified several logistical issues, and involved only one jurisdiction and three locations. Future remote kiosk voting projects would have to determine how logistical issues, such as travel and materials transport, scale in a more ambitious project. The extent of technical support will be an

[43] U.S. Department of Defense, Federal Voting Assistance Program. *The 2008 Okaloosa Distance Balloting Pilot Project.* Alexandria, Virginia, December 2012), 1.

[44] Ibid., 2.

important future consideration. Finally, future implementations of remote kiosk Internet voting – in particular, those that might have a larger scope and scale than the ODBP – will need to consider carefully how to recruit, staff, and train kiosk workers for overseas kiosk operations.

The standard operating procedures associated with the ODBP are important to address in any remote kiosk voting effort. Any remote kiosk project needs to have clear procedures for managing the chain of custody of all aspects of the remote kiosk voting process. Also, because post-election ballot audits are becoming an increasingly important mechanism for verification of the integrity of an election (and for ensuring stakeholder and voter confidence), it is critical to consider how to design and implement post-election ballot auditing in a remote kiosk environment.

Across all of these areas, it will be critical to the success of future efforts to design an effective evaluation of any system, including effective user and remote kiosk worker feedback components. It will also be imperative to conduct a comprehensive campaign to advertise the availability of the remote kiosk Internet voting option to maximize system use.

UNDERSTANDING REMOTE KIOSK VOTING BARRIERS

Given that the ODBP was the first implementation of a remote kiosk Internet voting system, having a description of the system was critical in determining future research needs associated with remote kiosk voting. The key report findings provided the basis for much of the other research conducted by FVAP on remote kiosk voting. Subsequent research focused on understanding the legal landscape in the States associated with remote kiosk voting.

The report *The Potential for Kiosk Voting in Nine States* examines the legal and regulatory barriers that may exist should FVAP desire to do a multistate kiosk voting effort. For this report, election officials in nine States – California, Florida, Hawaii, New York, North Carolina, Pennsylvania, South Carolina, Texas, and Washington – were surveyed regarding specific laws, policies, and procedures that had been critical to the success of the ODBP. State election officials were asked about (1) the "pilot friendliness" of their State, (2) testing and certification complexity, (3) the amenability of their State to electronic voting processes, or its "e-friendliness," and (4) polling place access. The local election officials surveyed were asked about (1) security requirements for a remote voting location, (2) chains of custody, and (3) requirements to be an election worker.

This study had several key findings:

- States tended to view the remote kiosk system as an early voting location – under State laws, the kiosk appears to be considered more like early voting than absentee voting.
- Given this view, the biggest barrier is that most responding States do not allow people from outside of their own State to be in a voting location. For example, most States do not allow individuals in a polling place unless they are registered to vote in the State and are there for the purpose of voting. Likewise, strict limitations exist in the laws of many of these States on the number of observers or watchers who can be in a polling location, and those laws could be violated in a multistate pilot.
- States would likely require legislative approval for any pilot.
- States would likely want the project to meet the EAC Voluntary Voting System Guidelines, or the EAC standards for Internet-based *UOCAVA* pilots.
- Some States have laws and regulations in place to allow e-voting, but those laws and regulations limit the use of networks or ballot transmission over the Internet.
- Finally, some States raised general reservations about participating in such a future pilot study.

Data received from local election officials also underscored the hurdles that future remote kiosk pilot projects might face. Issues of particular concern expressed from the States surveyed include:

- Many States have the explicit requirement that their election workers be registered voters in the State. This could create complications for multistate implementations.
- Some States require partisan balance among election workers.

This report provides key insights as to whether the ODBP project is reproducible across States and jurisdictions. It finds that, generally speaking, there are multiple barriers to implementing a multistate remote kiosk voting system, and several of these barriers may also exist across jurisdictions within a State. Although the report only covers nine States, it does cover almost all of the most populous *UOCAVA* States, so its findings are important in understanding the feasibility of a multistate pilot in the current legal environment.

Risk Assessment Studies

The VSTL and penetration test studies were intended to develop methodologies for evaluating specific aspects of the security of remote electronic voting systems. The CAC/DISN study and the kiosk voting study examined whether there were more secure platforms on which such voting could occur. These items are specific evaluations of security related to specific aspects of a remote electronic voting system. It is also important to examine these questions at a higher level, in the context of systemic risk.

Knowledge of the risks associated with any voting technology is a critical component of system development, implementation, and evaluation. The integrity of the voting process must be maintained at the highest level possible, so the legitimacy of a particular election will not be undermined by a voting system. It has also been critical for FVAP, as it sought to fulfill the congressional electronic voting demonstration project mandate, to know the potential risks associated with the various options for voter authentication, ballot transmission and return, and ballot tabulation to adequately assess the various technological options under consideration.

FVAP undertook a research project to develop a methodology that could assess the potential portfolio of risks that might be associated with various forms of electronic registration and voting solutions for *UOCAVA* voters.

Comparative Risk Analysis

In 2013, FVAP initiated a different form of risk analysis and threat evaluation in order to address the outstanding research question of how to quantify risks related to remote electronic voting and compare those risks to the existing postal-based *UOCAVA* voting system. This research is summarized in the report *Comparative Risk Analysis of the Current UOCAVA Voting System and an Electronic Alternative* (2013; hereafter, "CRA"). This analysis built on earlier efforts to develop methodologies for assessing threats to remote electronic voting systems, such as the qualitative threat and risk assessment analysis conducted as part of the SERVE project.[45] Similar to the SERVE threat assessment study, the CRA was an attempt to develop a framework and methodology for

[45] U.S. Department of Defense, Federal Voting Assistance, "Secure Electronic Registration and Voting Experiment: Threat Risk Assessment- Phase 3," v.0.5 (March 23, 2004). Retrieved from http://csrc.nist.gov/groups/ST/UOCAVA/2010/FVAP_SERVEThreatRiskAssessment.pdf

assessing potential threats to, and risks of using, an electronic voting system. The CRA differed in its ability to quantify these risks and provide a mechanism to compare relative levels of risk between two fundamentally different technologies or systems.

The CRA is similar to the qualitative approach used in the SERVE threat assessment analysis – both involve developing a framework and methodology for assessing risks to electronic voting projects – but does so through a very different approach. In particular, the SERVE approach used a qualitative risk assessment approach, and the CRA used a quantitative approach. Furthermore, the CRA applied the quantitative risk assessment approach in a comparative way, contrasting a potential electronic voting system's portfolio of potential risks to that of the existing voting-by-mail system that *UOCAVA* voters use. Finally, the CRA's approach to the estimation of risks generally comes from the perspective of viewing risks based on the means by which an attacker might attempt to hack the electronic voting system.

The approach used in the CRA is based on "threat trees," which are "… a data structure for representing the steps that an attacker would take to exploit a defect in order to accomplish malicious intent."[46] This approach relies upon mapping potential avenues of attack, and then classifying the likelihood and impact of each potential attack. As used in this report, the CRA process had the following steps:

- Review of 128 documents from the research literature on voting system risks and threats;
- Identification and classification of the risks and threats from this review into a threat tree analysis based on a model developed for the EAC;[47] and
- Development of a computational or simulation-based model to estimate the potential likelihood and impact of the identified risks.

This quantitative risk assessment approach was applied to an abstraction of the current *UOCAVA* by-mail absentee voting process (depicted in Sections 4.1.1 and 4.1.2 of the CRA report) in comparison to a hypothetical electronic absentee voting system (shown in Sections 4.2.1 and 4.2.2 of the CRA report). The comparison between the current by-mail absentee voting process and the electronic absentee voting process helps document the potential relative risks in the use of each different type of voting system for *UOCAVA* voters. The risk comparison between the two voting systems undertaken using this prototypical methodology asserted three substantive results: (1) "The current *UOCAVA* voting system appears to exhibit a greater risk from unintentional errors, while its electronic counterpart is equally subjected to attacks and errors." (2) "Security objectives are more affected by attacks in the context of the remote absentee voting system, and by errors in the context of the current *UOCAVA* voting system." (3) "Overall, the remote electronic absentee voting system and the current *UOCAVA* voting system exhibit similar risks, from a statistical viewpoint."[48]

The quantitative and comparative approach presented in the CRA report provides a significant advance and a useful framework that can be applied to voting technology development projects. If done well, this methodology for risk assessment could provide helpful information to better

---

[46] U.S. Election Assistance Commission, *Elections Operations Assessment: Threat Trees and Matrices and Threat Instance Risk Analyzer* (TIRA), (February 8, 2010), 1.
[47] The CRA references a 2009 version of the EAC document; however, there is a more recent version of this document that has been used as reference for this report, *Elections Operations Assessment: Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA)*, February 8, 2010.
[48] These conclusions can be found on page iii of the CRA report.

understand potential threats to any new approach that is being developed for *UOCAVA* registration and voting, but this approach also has some potential concerns.

There are three important components to the "threat tree" approach for risk assessment that are developed in the CRA report:

- The quality of the background research and data inputs;
- The expertise of the threat evaluation team and the process they use; and
- The assumptions behind the simulation model.

Although the CRA report is really only a pilot test for this approach to threat assessment, it is clear that each step of this process has serious concerns that must be addressed.

In the past 15 years, there has been a great deal of analysis of voting technologies – particularly, research that has been done by academics, election officials, and other experts – throughout the world. A great deal is now known about the reliability and risks associated with existing voting systems, including voting by mail. A thorough review and evaluation of this body of research would be necessary were the approach outlined in the CRA to be used for an electronic voting system for *UOCAVA* voters. However, although there is a great deal of research on existing registration and voting systems, the types of new technologies that might be under development for a future electronic voting system may be much more speculative and less well understood. Thus, the potential array of threats regarding these new electronic voting systems may not be well understood (or even understood at all). A methodology like this might not be able to model adequately unknown or poorly-understood threats to voting systems that have not been implemented repeatedly in real-world scenarios.

Next, this methodology needs a diverse and knowledgeable evaluation team. They have to sift through the known threats, analyze them, and provide the inputs for the simulation model. If the evaluation team is not staffed with knowledgeable members, or is missing critical expertise, then the inputs to the simulation model might be incorrect or poorly specified. Furthermore, the process that the evaluation team uses to evaluate risks and quantify their likelihood and significance is critical; if team members are not provided with sufficient time or resources, they might not provide the quality input data that the simulation model needs.

Finally, the simulation model is built on many assumptions; at the core is a Monte Carlo simulation approach that uses input values that are drawn from distributions identified in the evaluation stage and used to compute output probabilities. Although the range of technical assumptions that are used in a Monte Carlo simulation is quite large, it is important for any simulation like this to present the important assumptions in the simulation and discuss what robustness tests have been utilized to probe the importance of those assumptions. If assumptions made in the simulation process are incorrect, then the output from the simulation model may be misleading.

The comparative and quantitative approach outlined in the CRA report provides a foundation for future risk assessment that can be used for future *UOCAVA* electronic voting projects. Ideally, the CRA approach could be combined with the qualitative approach presented in the *SERVE Threat Risk Assessment* report. Together, the two approaches could provide a complementary set of frameworks for understanding risks and threats associated with any *UOCAVA* electronic registration and voting project, and identify specific areas that may require trade-offs when considering an actual remote electronic voting system architecture.

SUMMARY

Under the language contained in the NDAA FY 2005, FVAP was required to develop, test, and field an electronic voting demonstration project after the EAC adopted voting system standards for electronic absentee ballots and certified that it would assist DoD in this effort. To prepare for this requirement, FVAP evaluated the UPPTR as a baseline and developed tools to test a remote electronic voting system with respect to the UPPTR requirements. This work was conducted so that FVAP could assist with the development of relevant standards, initiate the process of anticipating such a system once the EAC completed development of voting system standards, and begin recognizing the supporting logistics and outstanding policy decisions.

The research deliverables discussed in Section 3 were intended to answer a specific set of research questions. The first set of research questions pertained to determining how to test a specific voting system or set of systems to ensure they conformed to appropriate accreditation standards, had robust security that could withstand sustained penetration testing, and met industry software assurance testing standards. The specific research questions are linked to primary deliverables in Table 3.1. It is important to note that most of the reports speak to more than one research question. For example, the penetration testing report addresses the specific penetration testing questions and the issue of conformance testing of the UPPTR.

In the absence of applicable standards at the time this research was completed, FVAP used the UPPTR to structure its system-specific evaluations of usability, security, and conformance. First, FVAP evaluated the usability aspect of the UPPTR in *Operation VOTE*. Second, FVAP developed a process for system testing based on the premise that FVAP would sponsor a form of certification testing to the relevant standards. The process that was developed in the VSTL report provided information that can be used to improve EAC standards for electronic absentee balloting. Third, processes for system security testing – specifically, penetration and software assurance – were developed and prototypes of these processes were tested to address concerns over software source code quality and how the process of source code review could be optimized for a completely software-driven voting solution.

Table 3.1: Research Questions and Deliverables Addressing System Integrity and Security

Research Question	Primary Research Deliverables
What type of FVAP-sponsored conformance test should be used to accredit these systems against the *UOCAVA* Pilot Program Testing Requirements (UPPTR)? What is the impact of this conformance test against the timeline for implementing a remote kiosk-based approach?	Recommendations for the UPPTR Voting System Testing Laboratory Functionality and Security Testing
What is the level of resistance existing systems possessed against penetrations? What is the eventual type of approach and methodology FVAP should consider for a large-scale implementation of a penetration test as part of its security posture?	Penetration Testing of a Simulated Election

Would the advent of software assurance tools hold value for identifying the extent of known defects in software source code? Could these tools be used to assist with source code reviews? What is the extent of coverage that software assurance tools could provide?	Investigation of the use of Software Assurance Tools on Internet Voting Software Applications

Second, FVAP conducted a set of studies related to the e*nvironment* in which any remote electronic voting demonstration project would occur. FVAP examined issues related to the use of DoD assets – specifically, its PKI infrastructure (CAC) and the NIPRNet – to fulfill the electronic voting demonstration project requirement. FVAP also considered whether remote kiosk voting was a viable model for remote electronic voting. Both analyses identified key barriers that would have to be addressed before either DoD infrastructure or kiosks were used as part of remote electronic voting initiatives. The specific research questions are linked to research deliverables in Table 3.2.

Table 3.2: Research Questions and Deliverables Addressing the System Environment

Research Question	Research Deliverable
What are the relative benefits/concerns with using the DISN as part of the overall architecture? Could the Department consider the use of a standardized client configuration as part of its remote electronic voting system? What would be the supporting logistics associated with this?	Voting Over the DISN-CAC Analysis Feasibility Evaluation
What is the role of the Department's CAC for system authentication purposes? What is the potential for its use as part of the voter authentication process?	Voting Over the DISN-CAC Analysis Feasibility Evaluation
What is the supporting statutory and legal framework for the States to participate in a remote kiosk-based pilot?	The 2008 Okaloosa Distance Balloting Pilot Project

Finally, FVAP conducted research that considers the overall risk environment in which any remote electronic voting demonstration project would be fielded. The goal of this research was to determine if there was an effective process by which the risk environment could be defined and then those defined risks could be quantified. The specific research questions are linked to the research deliverable in Table 3.3.

Table 3.3: Research Questions and Deliverables Addressing Quantifiable Comparative Risk

Research Question	Research Deliverable
What is the comparative level of risk between the existing postal-based system and that of a remote electronic voting system? Can this risk be quantified?	Comparative Risk Analysis of the Current UOCAVA Voting System and an Electronic Alternative

The tools developed were intended for refinement over time, but as discussed in these reports, could serve as a basis for a state or local government to test a voting system or recognize tradeoffs when developing the elements of a voting system.

SECTION 4: CONCLUSIONS AND RECOMMENDATIONS

FVAP's work related to remote electronic voting was largely driven by congressional requirements. Specifically:

- In the NDAA FY 2002, FVAP was charged with conducting an electronic voting demonstration project that would allow "absent Uniformed Services voters…to cast ballots in the regularly scheduled general election for federal office for November 2002 through an electronic voting system," and allowed the demonstration project to be delayed until 2004.
- In 2004, Congress passed the NDAA FY 2005, and section 567 of the Act removed the requirement of a demonstration project in 2004. Instead, FVAP was to conduct such a pilot in "the first regularly scheduled general election for federal office which occurs after the Election Assistance Commission 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."
- In December 2014, the requirement for FVAP to conduct a demonstration project was rescinded in the NDAA FY2015.

The enactment of the first requirement to conduct an electronic voting demonstration project opened up a new research agenda for FVAP. In addition to meeting its core mission activities, FVAP began to identify how it could meet the electronic voting demonstration project requirement. The language of the NDAA FY 2005 created a very short time frame for FVAP to implement any demonstration project. Once the EAC established electronic absentee voting guidelines, FVAP would have, at the very maximum, two years to carry out the demonstration project. In order to support this aggressive timeline, FVAP initiated the research studies discussed in Section 3 to examine the potential for a remote kiosk-based approach or a commercial solution for full remote electronic voting.

Table 4.1 lists all of the reports included in this study. This section provides overall recommendations based on the totality of these studies. Please note, each finding and recommendation included within each of these studies reflect assessment from the contractors who conducted the research, not from FVAP. Therefore, these recommendations should be considered, but each specific recommendation may not reflect the official position of FVAP, given that these studies were received and executed as individual research initiatives to address specific questions.

The findings and recommendations of any given report have to be considered in conjunction with those contained in the other reports. The integration of these reports into an actual operational model did not occur, because the electronic demonstration project requirement was repealed. Given the level of investment made through the use of public funds and the length of time associated with the original demonstration project requirement, FVAP thinks that the research, associated tools, and identification of the outstanding questions are valuable and should be built upon by interested parties at the federal level and considered by State and local election officials prior to moving forward with any remote electronic voting pilot.

Table 4.1: Research Conducted by FVAP Related to Remote Electronic Voting

Title	Date
Recommendations for the *UOCAVA* Pilot Program Testing Requirements (UPPTR)	02 November 2012
Federal Voting Assistance Program (FVAP) Operation VOTE	16 September 2011 (Publicly Available)
Voting System Testing Laboratory Functionality and Security Testing	11 November 2011
Voting System Testing Laboratory (VSTL) Appendix A – Glossary	No Date
Voting System Testing Laboratory (VSTL) Appendix B: UOCAVA Pilot Program Testing Requirements	25 August 2010
Voting System Testing Laboratory (VSTL) Appendix C – VSTLs' Comments to the UPPTR	No Date
Voting System Testing Laboratory (VSTL) Appendix D – Changes to the VSTL Standard Testing Methodology for UPPTR	No Date
Voting System Testing Laboratory (VSTL) Appendix E: SLI Global Solutions Test Report	19 July 2011
Voting System Testing Laboratory (VSTL) Appendix F: Wyle Laboratories Test Plan and Test Report	14 April 2011
Penetration Testing of a Simulated Election	16 September 2011
Penetration Testing of a Simulated Election, Appendix A – Air Force Institute of Technology, Penetration Test of Simulated Election Test Report	10 August 2011
Penetration Testing of a Simulated Election, Appendix B – CALIBRE Systems/RedPhone, LLC Federal Voting Assistance Program Voting Penetration Test	15 August 2011
Voting Over the DISN-CAC Analysis Feasibility Evaluation	5 October 2012
Investigation of the use of Software Assurance Tools on Internet Voting Software Applications	16 May 2014
The 2008 Okaloosa Distance Balloting Pilot Project	December 2012
The Potential for Kiosk Voting in Nine States	March 2013
Secure Electronic Registration and Voting Experiment, Threat Risk Assessment – Phase 3	March 23, 2004
Comparative Risk Analysis of the Current *UOCAVA* Voting System and an Electronic Alternative	28 February 2013

Conclusions From Research Findings

The research undertaken by FVAP in preparation for conducting a remote electronic voting demonstration project has led to the following conclusions. FVAP intends these conclusions as a cohesive set and any actions taken based upon them should reflect all of the conclusions and viewed within the overall context of the research. No single conclusion should be viewed in isolation.

- As the research conducted in response to the NDAAs for Fiscal Years 2002 and 2004 reveals, there are many questions about the appropriate role of the Federal Government in the development and implementation of a centralized voting architecture given the structure of election administration in the United States. For example, research on kiosk voting found that variations in State laws related to polling places make the conduct of a multi-jurisdictional remote kiosk voting effort difficult. Likewise, research on DISN/CAC showed how the boundaries between federal and State systems and networks have to be carefully understood and clarified prior to fielding such a system. The ever-changing threat environment for information systems warrants a clear line of accountability that became blurry by the time FVAP's research concluded.

  There are many logistical and information security reasons for looking to FVAP to be a part of remote electronic voting pilots for the *UOCAVA* population. However, in order for FVAP to address these logistical and security concerns any notional voting system would require more centralized authority which would mitigate certain security risks, but could raise policy issues, as well. Any time DoD is viewed as being part of the historically State-centered role of ensuring the integrity of voted ballots processed through the system it can raise questions about the control of the voting process in a State and the eventual sequence of events should a federal election be contested before the Courts.

- A remote kiosk voting system at present is not a tenable solution for serving the *UOCAVA* population. Implementing a kiosk system that served more than a single election jurisdiction in a single State would be complex. First, as the report *The Potential for Kiosk Voting in Nine States* noted, all States studied in regard to kiosk voting had laws that would have impeded the implementation of a multi-jurisdictional kiosk voting pilot project. Second, the security requirements for military installations, the lack of PKI-based credentialing for civilians, and other factors would limit the ability of civilians to participate in a kiosk voting initiative. Finally, under most kiosk-voting scenarios that would fulfill the remote electronic voting demonstration project requirement, the Services would be in a position of managing polling locations for States and localities, which is not expressly authorized.

- FVAP's work on software assurance created a methodology for testing source code and identification of defects. The FVAP-developed software assurance approach – along with the penetration testing and usability testing models proposed – could be the basis of a dynamic approach that could to evaluate and improve upon any remote electronic voting solution. To remain relevant, research conducted on threat and risk assessment, penetration testing, and intrusion detection must be continuously adjusted to address the current and future security environment.

- The software assurance tools used as part of this initiative successfully tested and identified software defects as true positives. The use of multiple tools added marginal value to the number and scope of positive defects, but more research is required on the exact combination of tools that yield the most effective level of detection. It is important to note that merely identifying defects does not provide an overall assessment of a system's security posture. Rather, the identification of defects necessitates a deeper level of code examination to determine the true nature of the risk and context.

- Comparative risk analysis – and an appreciation of the risk environment – is critical for the success of any remote electronic pilot as it will drive not only a consensus approach to

understanding the inherent threats through a consensus approach, but it will also inform the potential tradeoffs that should occur when considering system development in order to inject no more significant risks than the existing system. A comparative risk analysis should involve an array of computer security and election administration experts and should be seen as a means to provoke active discussion and collaboration.

- Any remote electronic voting pilot will take time to implement; two years was not an adequate period to test, remediate, and field such a system. The research conducted by FVAP found that, before any remote electronic voting pilot is fielded, the system will have to undergo extensive risk assessment modeling, including voting system standards testing, software assurance testing, penetration testing, usability testing, and conformance testing. These tests, and the remediation that would be required of any system before it completed all of these tests, would clearly take longer than two years. Even once this process was complete, the time required to field and advertise such a system to *UOCAVA* voters would be substantial.

FVAP's research and the recommendations listed above have specific implications for FVAP moving forward:

- FVAP can best serve its constituency by focusing on its core mission. FVAP is a service organization, with three primary functions: (1) informing *UOCAVA* citizens of their right to vote and assisting them as they exercise their right to vote (2) assisting the States in complying with relevant federal laws by providing current information, and (3) working with State and local election officials on behalf of *UOCAVA* voters to identify impediments to their ability to exercise their right to vote, and methods to overcome those impediments.

  FVAP is best suited to helping election jurisdictions understand the challenges faced by UOCAVA voters and explain how their processes and/or systems may serve or hinder *UOCAVA* citizens.

- Should the EAC and NIST decide to refine standards for remote electronic voting and look to apply this research, FVAP will be available to assist with these efforts. FVAP thinks that the research noted in this report could provide a basis for continuing to improve existing standards and would be able to provide additional background information regarding the research it has already conducted to help these agencies.

  FVAP can also help State and local governments understand the research discussed in this report should they wish to apply this research.

FVAP initially took on a central role in the implementation of demonstration projects in order to successfully mitigate the vast majority of security concerns. However, a federally centralized system creates a potential point of vulnerability for the voting system, and creates an opportunity for controlling an overall network and monitoring the network for client conformance and system intrusions. This is a relevant point of interest for all election community stakeholders as our level of awareness in the area of information security is fundamentally different from fifteen years ago.

Thus, a State-run, but FVAP-supported, set of voting systems – that are tested against State and federal standards and certified for use by the participating States – would distribute risks across States and better reflect the current administrative and legal framework for conducting elections in the United States. Ultimately, FVAP is pleased with the research it conducted as part of its efforts to

meet the requirement for the conduct of an electronic voting demonstration project. DoD is no longer exploring program implementation in this area. However, with the level of investment made through the use of public funds and the length of time associated with the original demonstration project requirement, FVAP believes that the research, associated tools, and identification of the outstanding questions are valuable and should be shared with the *UOCAVA* stakeholder community. Should a State or federal agency determine it wishes to pursue a full or partial Internet voting solution, it should do so in a fashion that takes advantage of the knowledge gleaned from FVAP experiences and these extensive research efforts.