Internet Voting Revisited:

Security and Identity Theft Risks of the DoD's Interim Voting Assistance System

David Jefferson, Avi Rubin, Barbara Simons, and David Wagner
info@servesecurityreport.org

October 25, 2006

Background

In 2004 the Defense Department Federal Voting Assistance Program (FVAP) built and intended to deploy a voting system called SERVE, the Secure Electronic Registration and Voting Experiment, designed to help military personnel and overseas civilians to register and vote in the primary and general elections of that year. As members of an external peer review panel for SERVE, we published a report entitled "*A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE),"* available at http://servesecurityreport.org. In the report we identified a large number of security risks and vulnerabilities, including denial of service attacks, insider attacks, viral attacks on voters' PCs, and many others. Shortly after publication of the report, the DoD terminated the program, citing security concerns.

We recently learned that FVAP has created a new online system, the Interim Voting Assistance System (IVAS). IVAS has a similar mission, namely to aid military personnel and overseas civilians to register and vote in the coming November 7 general election. In this short paper we present our serious concerns about the security issues posed by this new system.

None of these security concerns is original; all were raised in a DoD internal review, discussed below.

IVAS was announced to the public only last month (September)[1], and has been designed and built only over the last several months[2], an extremely short time for a system of this complexity and

---

[1] "On September 5, 2006 the Principal Deputy Undersecretary of Defense for Personnel and Readiness and the FVAP Director and Deputy Director participated in a round-table press conference announcing both IVAS 2006 and the 2006 Armed Forces Voters Week". From page 7 of "Report on the Status of the Interim Voting Assistance System (IVAS) Ballot Request Program", September 2006, http://accurate-voting.org/wp-content/uploads/2006/10/ivas.pdf.

[2] "The legislation that required a continuation of IVAS was enacted on June 15, 2006 and work commenced immediately toward a successful launch date of September 1, 2006 for a total of 79 days." This was the response to question 6 about the length of the development cycle from Representative Maloney, available at http://accurate-voting.org/wp-

importance. The current system has never been used in a public election before (not even in a primary), and has not been subject to any publicly available external security examination. The technical specifications have not been made publicly available.

An internal security review.

An internal review done for the DoD has raised serious security questions about IVAS. The following is from page 9 of the *Independent Review Final Report for the Interim Voting Assistance System (IVAS)*[3]:

> Security Concern.
>
> The transmission of voting materials by unsecured e-mail is a concern from both a privacy and security concern. E-mail traffic can flow through equipment owned and operated by various governments, companies and individuals in many different countries. It is easily monitored, blocked and subject to tampering. In addition, the publication of e-mail addresses of voting officials subject those offices to attack, effectively blocking voters.
>
> E-mails can be easily and reliably signed and encrypted to reduce the risk of tampering. If LEO [Local Election Official] servers are configured to only accept signed communications, it will also reduce the risk of a "spam" attack. However, at the time of this report, there is no plan to digitally sign or encrypt e-mail communications.
>
> Security risk for the current FVAP/DMDC [Defense Manpower Data Center] e-mail effort is not a direct DoD or FVAP liability as the voter communication is direct between the voter and the LEO. However, the risk that tampering could occur is significant and may reflect negatively on FVAP or DoD.

It is disturbing that the DoD did not heed warnings about the security risks of IVAS from its own internal review. Furthermore, the letters sent to the states did not warn them that they are participating in the program with intrinsic security risks[4]. In fact, the DoD labeled the internal review document as "Official Use Only" by inserting the following statement at the bottom of each page:

> SENSITIVE WORKING PAPERS - FOR OFFICIAL USE ONLY. The information contained herein may contain sensitive and pre-decisional Department of Defense information and is protected from mandatory disclosure under the Freedom of Information Act (FOIA), 5 USC552. Do not forward outside of the Department of Defense without the expressed permission of the originator.

---

content/uploads/2006/10/IVAS-UnderSecDef.pdf

[3] We downloaded the report from a publicly available website: http://www.nationaldefensecommittee.org/files/IVAS_FINAL.pdf

[4] "We encourage you to make available as many of these electronic transmission alternatives as possible to your UOCAVA citizens". From a letter to Ms. Jean Jensen, Secretary, State Board of Elections, Richmond, VA. The letter is dated July 25, 2006 and signed by P. K. Brunelli. It is Exhibit 1 (page 11) in the status report referred to in footnote 1.

Finally, we note that for service people stationed abroad, email and fax transmissions are being routed through the phone systems of the country in which they are stationed. We have enough problems trying to secure telecommunications within the US. Clearly, the DoD cannot guarantee the security of telecommunications from within another country.

A description of the system.

Based on a status report by David S. C. Chu, Under Secretary of Defense, dated September 2006[5], the following is a rough description of the options being deployed. Chu refers to Solution One and Solution Two. Other documents refer to Tool One and Tool Two, but the difference appears to be just in the names used. Tool One was built by an internal DoD development group (the Defense Manpower Data Center); Tool Two was built by private contractors using "private R&D funding and volunteer time from the developers."[6]

Tool One:

1. After logging in over the public Internet using a unique DoD number, the voter fills out an online version of a voter registration form (referred to as the FPCA or Federal Post Card Application), the voter completes the form, saves it to the local disk, and emails it as an attachment (without signature) directly to the LEO (local election official) as a PDF attachment.
2. The LEO then sends a blank ballot to the voter via email, fax, or snail mail, "in accordance with state law".
3. Nothing more is said, but we also know that the voter can return the voted ballot by email, fax, or snail mail, depending on what the state will accept. This process is facilitated by the FVAP through their Electronic Transmission Service (ETS).

Tool Two:

1. After logging in over the public Internet using a unique DoD ID, the voter completes and saves an automated version of the FPCA onto an SSL enabled server. The document does not describe how the voter fills out the FPCA or the format of the saved version.
2. The LEO logs onto the DoD server over SSL and downloads the completed FPCA.
3. The LEO posts a PDF of the blank ballot onto the DoD server, and the voter downloads and prints the ballot.
4. Same as number 3 above.

Voted ballot confidentiality.

The FVAP claims in several responses to questions asked by Representative Maloney that IVAS does not facilitate the electronic submission of voted ballots, but rather is being used only to allow service people to register to vote and, in the case of Tool 2, to obtain a copy of a blank ballot[7]. For example, in response to Question 4 asking about system specifications and a complete project description, the following answers are given. Regarding Tool One: "Neither the

---

5 http://accurate-voting.org/wp-content/uploads/2006/10/ivas.pdf

6 From the Independent Final Review, page 6.

7 http://accurate-voting.org/wp-content/uploads/2006/10/IVAS-UnderSecDef.pdf

blank ballot nor the voted ballot is transmitted by [Tool One]." Regarding Tool Two: "The voted ballot does not go back through the secure server". Similar claims are repeated in response to several other questions. In response to Question 12A, the answer says, "The IVAS tools provided to the state will not facilitate the electronic submission of voted ballots. Citizens can consult the Integrated Voting Alternative Site state page and Voting Assistance Guide (VAG) located on the FVAP website to ascertain what electronic alternatives their state allows for the submission of a voted ballot."

While this is literally true of the IVAS software, the FVAP clearly is facilitating and encouraging voting via email or fax. According to an article in *Computerworld* that quoted J. Scott Wiedmann, deputy director of FVAP[8]

> The program … provides instructions for personnel on how to submit local ballots by fax machine or e-mail.

States were also informed of FVAP support for voting via email or fax, as is illustrated by the following quote, contained in a letter[9] to Jean Jensen, Secretary, State Board of Elections, Richmond, VA:

- Consider a faxing/email option for return of voted ballots. If your state currently does not allow voting materials to be transmitted via email, but does allow faxing, FVAP has enhanced its Electronic Transmission Service to receive faxed voting materials and forward them as email attachments. This option will provide a viable alternative to Uniformed Service members stationed in combat zones and other overseas areas. Due to the security measures taken by the military, the capability for unclassified fax transmission is not available to most of our service members in these regions, but email transmissions are an option for many. After receiving an email from Uniformed Service members and other overseas voters, FVAP can forward the transmission to the states as a fax document to comply with state law.

In other words, the voter sends his or her voted ballot via email to the DoD, which downloads it, scans it, and then transmits the email as a fax to the LEO. Not only is there no ballot confidentiality for the voter, but also the opportunities to manipulate the ballot are obvious. In such a system there is no way to provide effective oversight and no provision for outside observers.

The use of faxes or email requires that the voter give up his or her right to a confidential ballot. While it is disturbing that any voters are being asked to give up their right to a confidential ballot, it is even worse when that right is being lost in a hierarchical organization such as the military.

Identity theft and vote tampering.

Another risk to the voter is that of identity theft. With Tool One, personally identifiable

---

[8] *New Military Voting Process Lacks Security, Critics Say*, by Marc Songini, October 16, 2006, http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=legislation_regulation&articleId=268797&taxonomyId=70&intsrc=kc_top

[9] Page 13 of the Chu document.

information for voter registration is sent via unencrypted email over the Internet. The FPCA lists the following information as required, even though some of the information (e.g. race) may not be required by the state in which the service person will be voting: name, sex, race, date of birth, social security number (SSN), state driver's license or I.D. number, telephone number, fax number, email address, voting residence, and preference for ballot format (mail, fax, or email). Only political party preference is listed as optional on the FPCA.[10]

Risks.

In summary, we see three main risks:

1. Tool One exposes soldiers to risks of identity theft. Sending personally identifiable information via unencrypted email is considered poor practice. No bank would ask their customers to send SSNs over unencrypted email, yet Tool One does exactly that. This problem is exacerbated by potential phishing attacks.
2. Returning voted ballots by email or fax creates an opportunity for hackers, foreign governments, or other parties to tamper with those ballots while they are in transit. FVAP's system does not include any meaningful protection against the risk of ballot modification.
3. Ballots returned by email or fax may be handled by the DoD in some cases. Those overseas voters using the system sign a waiver of their right to a secret ballot. However, it is one thing for a voter's ballot to be sent directly to their local election official; it is another for a soldier's ballot to be sent to and handled by the DoD – who is, after all, the soldier's employer.

What might be done.

We sympathize with the problems that service people have with registering, obtaining a ballot, and getting the voted ballot to their LEO in time for the ballot to be counted. However, given the current state of technology, it is not wise to send voted ballots or personally identifiable information over unencrypted email or fax. We agree that something should be done. But it should never be done while also exposing the voter to the risk of ballot manipulation or identity theft – risks about which the voter might be completely unaware.

We support exploring the possibility of using the Internet to enable overseas voters to request ballots (by filling out and securely transmitting an electronic FPCA) and to deliver blank ballots to these voters – if the system and procedures are implemented securely. It is unfortunate that the DoD didn't create a system that focuses solely on ballot requests and blank ballot delivery, without including other risky and questionable practices.

Regardless of how blank ballots are distributed, voted ballots should be returned only via postal mail. Special steps should be taken, if necessary, to ensure that mailed ballots are picked up and mailed in a timely fashion so that they arrive in time to be counted. We know that the FVAP does a lot of work to ensure that military postal systems are moving ballots as fast as possible. Such action is laudable and should continue.

Tool One, which uses unencrypted email to send personally identifiable information, falls short of security practices in widespread commercial use. Banks and electronic commerce sites routinely

---

[10] http://www.fvap.gov/pubs/onlinefpca.pdf

provide this level of protection for their customers. We believe that overseas voters deserve at least as much protection when they vote as when they purchase a book from Amazon.

In conclusion, IVAS should have been subjected to an in-depth external review by independent security experts before being deployed. Our service people should not be voting on a system that creates risks of identity theft, hacking, and vote tampering and which requires voters to relinquish their right to a secret ballot.