Testimony of Ellen Theisen on H.B.1624, February 6, 2009

The National Institute of Standards and Technology (NIST), the U.S. Government Accountability Office, and dozens of professional computer security experts warn that the safe use of the Internet for voting is essentially impossible, given the technology available today.

- **In 2004, a panel of experts commissioned by the U.S. Department of Defense** concluded that it was not possible to ensure the privacy, security, or accuracy of votes cast over the Internet with its current architecture. They said the attempt to provide secure, all-electronic Internet voting was "an essentially impossible task."[1]
- **In 2007, the U.S. Government Accountability Office (GAO)** found that email and Internet voting is "more vulnerable to privacy and security compromises than the conventional methods now in use" and that "available safeguards may not adequately reduce the risks of compromise."[2]
- **In 2008, the National Institute of Standards and Technology (NIST)** wrote, "Technology that is widely deployed today is not able to mitigate many of the threats to casting ballots via the web."[3]
- **In 2008, thirty leading computer science experts and professors at major universities** signed a statement asserting that until "serious, potentially insurmountable, technical challenges" are overcome, permitting the Internet to be used for public elections "is an extraordinary and unnecessary risk to democracy."[4]

In their 2004 report, the panel of experts commissioned by the Department of Defense to evaluate the DoD's Internet voting project addressed a commonly asked question in the section entitled "Why security for Internet voting is far more difficult than for e-Commerce." They said:

> Many people mistakenly assume that since they can safely conduct commercial transactions over the Internet, that they also can safely vote over the Internet. First, they usually underestimate the hazards of online financial transactions, and are unaware of many of the risks they take even if they are careful to deal only with "secure" web sites through the SSL protocol. But they also assume that voting is comparable somehow to an online financial transaction, whereas in fact security for Internet voting is far more difficult than security for e-commerce. There are three reasons for this: the high stakes, the inability to recover from failures, and important structural differences between the requirements for elections and e-commerce.

---

[1] "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)." January 20, 2004. By Dr. David Jefferson, Dr. Aviel D. Rubin, Dr. Barbara Simons, Dr. David Wagner. http://www.servesecurityreport.org/

[2] "Action Plans Needed to Fully Address Challenges in Electronic Absentee Voting Initiatives for Military and Overseas Citizens," June 2007, p. 30. [GAO Report 07-774] http://www.gao.gov/new.items/d07774.pdf

[3] "A Threat Analysis on UOCAVA Voting Systems." [NISTIR 7551] http://vote.nist.gov/uocava-threatanalysis-final.pdf

[4] "Computer Technologists' statement on internet voting." September 11th, 2008. http://www.verifiedvoting.org/article.php?id=5867

They explain the structural differences these three reasons require, and they conclude.

> There are no such requirements for e-commerce systems. In general, designing an Internet voting system that can detect and correct any kind of vote fraud, without issuing voters receipts for how they voted, and without risking vote privacy by associating voters with their votes, is a deep and complex security problem that has no analog in the e-commerce world. For these reasons, the existence of technology to provide adequate security for Internet commerce does not imply that Internet voting can be made safe.

The NIST report provides a detailed list of threat to the various types of electronic and Internet voting, assessing the aspect of an election that is threatened, the risk level of each, and the difficulty level of threat. The report summarizes its threat analysis of the three electronic methods of transmitting election materials – fax, email, and Web-based Internet voting – and concludes that the threats to returning voted ballots by fax can be mitigated by proper procedures. But regarding the return of ballots via the Internet, NIST says,

> "The security challenges associated with e-mail return of voted ballots are difficult to overcome using technology widely deployed today." and
>
> "Technology that is widely deployed today is not able to mitigate many of the threats to casting ballots via the web."

In its suggested next steps, NIST says:

> "The threat analysis documented in this paper identifies blank ballot distribution methods as a potential area to immediately improve UOCAVA voting without threatening the security of elections. Fax, e-mail and web-based systems could distribute blank ballots quickly and reliably to voters, significantly reducing the ballot delivery times faced by mailing ballots to voters and improving the UOCAVA voting experience for citizens overseas. In addition, registration and ballot requests can also take advantage of these distribution methods, but there are more threats when handling personal information from voters."

A report from the Pew Center on the States, released last month found that Washington State was one of 25 states where military and overseas voters had time to vote. The Pew report points out that Washington State has already implemented the next steps that NIST suggests, and that the state already provides the 45 days transit time recommended by the DoD's Federal Voting Assistance Program (FVAP). In other words, Washington State is already providing well for its UOCAVA voters, without taking the severe risks associated with returning voted ballots through the Internet.

H.B. 1624 is a solution in search of a problem, and the solution it proposes would put at risk the privacy and votes of the very voters it is seeking to protect.

It is important to point out that the federal government has not been able to protect its own networks from cyber attacks. The Department of Homeland Security spent $6.6 billion dollars in 2008 on programs to secure the Internet networks of the Pentagon and other military computers, many of which house classified or sensitive information.[5]

[5] http://www.dhs.gov:80/xnews/releases/pr_1207684277498.shtm

However in November 2008, a serious attack on the Pentagon was successful: [6] [7]

> The Pentagon has suffered from a cyber attack so alarming that it has taken the unprecedented step of banning the use of external hardware devices, such as flash drives and DVD's.
>
> The attack came in the form of a global virus or worm that is spreading rapidly throughout a number of military networks.
>
> A Navy rear admiral outside the Pentagon, in a briefing to his staff on Thursday, characterized the virus as a coordinated attack that was strategically timed to hit between the Nov. 4 presidential election and Inauguration Day, Jan. 20.

Furthermore, the federal Department of Defense has been unable to meet Congress's expectation "to establish a secure and private electronic and Internet-based UOCAVA voting environment."[8] The GAO report says that, "the DoD has not developed a secure, Internet-based absentee voting demonstration project, as Congress mandated in the Ronald W. Reagan NDAA [National Defense Authorization Act] for Fiscal Year 2005."[9]

It is unrealistic to expect the Washington Secretary of State – on the State's limited budget – to accomplish something the United States Department of Homeland Security and the Department of Defense have been unable to accomplish with their billion dollar budgets and under the mandate of Congress.

I urge the legislature to take NIST's suggestion regarding the return of voted ballots via the Internet:

> "Voted ballot return remains a more difficult issue to address, however emerging trends and developments in this area should continue to be studied and monitored."

Alter H.B. 1624 to authorize the Secretary of State to form a task force of qualified computer security experts to study and monitor developments in Internet security.

The intent of Congress in passing UOCAVA was that:

> "all eligible American voters, regardless of race, ethnicity, disability, the language they speak, or the resources of the community in which they live, should have an equal opportunity to cast a vote and to have that vote counted."[10]

It is unfair to our military and overseas voters to offer them a means of voting that presents such a severe threat to the privacy and integrity of their ballots that NIST, the GAO, and computer security professionals across the country are warning against it. I urge you to defeat this seriously defective bill.

Ellen Theisen
660 Jefferson Ave.
Port Ludlow, WA 08365
360-437-9922

---

[6] "Pentagon Hit by Unprecedented Cyber Attack." FOXNews.com. November 20, 2008. http://www.foxnews.com/politics/2008/11/20/pentagon-cyber-siege-unprecedented-attack/

[7] "Military Looking Abroad for Source of Cyber Attack on Pentagon." FOXNews.com. November 21, 2008. http://www.foxnews.com/politics/2008/11/21/source-cyber-attack-pentagon-come-china/

[8] GAO Report 07-774, page 31 (pdf page 35) http://www.gao.gov/new.items/d07774.pdf

[9] GAO Report 07-774, page 27 (pdf page 31)

[10] http://www.usdoj.gov/crt/voting/42usc/subch_ig.php