Comments by Meg Holmberg to the

San Francisco Voting Systems Task Force

June 15, 2011

Hello.

My name is Meg Holmberg. I'm here as a citizen who for the past 7 years — since the election of 2004 — has been educating myself about threats to the integrity of our elections. I'm also a member of the Voting Rights Task Force, and a former co-chair for that group.

My comments to the Task Force have to do with Finding #5 on page 26. I'd like to point out that, as it now reads, this finding is inconsistent with — you might even say contradictory to — the wording of Finding 8.

Right now, Finding 5 reads this way:

“U.S. overseas and military voters could be better served with a digital means of voting.”

However, Finding 8 states that:

"...the use of remote digital voting—especially the digital return of voted electronic ballots with no audited paper ballots—is far too insecure in public elections application for the foreseeable future."

Before the Task Force finalizes your report, I strongly urge you to revise Finding 5 to specifically exclude the electronic submission of voted ballots by US overseas and military voters. Here is why I think this is so important.

Over the past few years, I've seen a growing interest in the idea of voting using the Internet — from personal computers, cell phones, or remote kiosks — particularly among people who want to ensure that members of the military serving overseas are able to vote. In many state legislatures, including California, bills have been introduced to make this possible.

To understand the dangers that Internet voting would pose to our elections, I'd like to bring to your attention comments made by Dr. David Jefferson, a Senior Scientist at Lawrence Livermore Labs whose job it is to devise strategies to defend against the daily attacks on U.S. computer networks, both government and corporate. Dr. Jefferson has served as a voting technology advisor to five successive Secretaries of State in California, and he was a co-author of the best known peer-reviewed scientific publication on Internet voting, the SERVE Security Report, which was commissioned by the Department of Defense. The organization of computer scientists known as Verified Voting says on its website: "It is likely that no one in the country has studied the subject of Internet voting more intensely than David Jefferson."

In late 2009, Dr. Jefferson testified before the Federal Communications Commission. Here's what he had to say about Internet voting. I'm giving you just a few key excerpts. His full comments are available online at http://fjallfoss.fcc.gov/ecfs/comment/view?id=6015502226.

> "I have several concerns about the security of Internet voting, based on my long study of the subject and on the well-known vulnerabilities inherent in the architecture of the Internet...
>
> "The worst security nightmare would be to allow voting from voters' own PCs or smart phones, or any other unsecured terminal node on the Internet or telephone network. (This includes all web-based voting, email voting, fax voting, phone voting, etc. and any hybrids.) At the technical level I am talking about, they are all exceedingly dangerous, with email and fax being a worst of all. There are so many kinds of attacks that can corrupt such an election that the mind boggles..."

After detailing these kinds of attacks, Dr. Jefferson goes on to say:

> "You will no doubt hear from vendors, lobbyists, and other financially interested parties that Internet voting can be made secure. Please, I implore you not to accept these claims without consulting independent experts in network and voting security..."
>
> "You may well hear claims that strong voter authentication or sophisticated cryptography can and do routinely secure public online elections. Please listen to the independent experts who will tell you that no amount of authentication and no (known, vetted) crypto protocol can do this. These claims of security are false..."
>
> "You may hear claims that many elections and election pilots have been conducted in the past without the loss or mis-recording of a single vote. This claim is false on several levels..." (He goes on critique these claims.)

Then he talks specifically about overseas military voting:

"Some people argue that the barriers to voting faced by our overseas military are so high that they justify, or require, online voting as the only reasonable solution. While it is true that those barriers are indeed unconscionably high, it is not true that there are no other good solutions besides Internet voting. We can go a long way toward reducing those barriers by carefully implementing Internet-based voter registration systems, and by using the Internet to distribute blank ballots electronically**. But we really must draw the line at permitting the electronic return of voted ballots.** That is the stage of the voting process at which all of the critical security dangers are concentrated, and **there is no good solution at this time, nor is there likely to be in the foreseeable future**." *(Emphasis mine.)*

Dr. Jefferson concludes:

"If I might make only one recommendation, it would be to not accept any claims regarding Internet voting security, reliability, or scalability, without consulting independent experts who have studied the issues, experts from both the academic and the national security/intelligence communities."

Thank you for your time.