Dear VSTF:

I would like to make the following suggestions with respect to your June 1, 2011 draft.

In section "2.2.3.2 Ballot Marking and Casting", I suggest that you change the paragraph that begins "There is significant controversy regarding the security risks of any remote digital voting" (lines 8 - 16 on my copy of the June 1 draft) to read as follows:

The use of the Internet for returning voted ballots represents a national security issue. Anyone with Internet access, including hostile nation-state actors, organized crime, disgruntled individuals, or political parties, may carry out attacks against Internet voting systems. In 2010, when the District of Columbia's pilot Internet system was penetrated by University of Michigan scientists, the team observed attempts to break into the system that were coming from Iran and China. While most attacks on systems permitting electronic return of voted ballots will be undetectable, even detected attacks are likely to be irreparable. An Internet voting system is exposed to a vastly greater number of security risks than a polling-place machine.

In addition, voters transmitting ballots over the Internet are asked to waive the privacy of their ballots, because ensuring that privacy is an unsolved problem. Significant effort has been expended to find ways to ensure that any and all voters can vote privately and independently. Asking certain groups of voters such as those in the military to waive secrecy in order to vote, as is currently done when ballots are returned electronically, undermines the right of all American voters to secret ballot elections and the benefits that accrue thereto.

Major Internet structural vulnerabilities have led computer security experts to caution against its use for returning voted ballots until at least such time as those vulnerabilities have been satisfactorily addressed. Organizations with security expertise dwarfing that of any voting system vendor or election jurisdiction - Google, Symantec, and the White House, to name a few - have all been victims of remote attacks. We cannot expect a vendor's or election jurisdiction's network to resist remote attack.

We support the responsible use of technology where it can benefit voters, while opposing technology that makes our elections highly vulnerable to rigging.

I omitted the reference to the Okaloosa County project, both because it is not obvious how it would scale up and because there were some problems. However, if you really want to refer to Okaloosa, then I suggest you include the following paragraph from the review of the Scytl voting software, used in Okaloosa County. The review was done by a team of outside experts, commissioned by the State of Florida as part of the state certification process.[footnote: Michael Clarkson, Brian Hay, Meador Inge, Abhi Shelat, David Wagner, and Alec Yasinsac, "Software Review and Security Analysis of Scytl Remote Voting Software", September 2008,
http://election.dos.state.fl.us/voting-systems/pdf/FinalReportSept19.pdf].
The team included computer security expert Alec Yasinsac, who worked with Operation Bravo in the design of the system. One of their findings was:

> The system is vulnerable to attack by trusted insiders (such as
> election officials behaving maliciously). Defending against such
> attacks can be challenging in any voting system. In Scytl's system,
> Voter Choice Records are pivotal to this defense. Manual counts of the
> Voter Choice Records, as well as procedural controls on insider access
> to the system before and during an election, are the only way we have
> identified to secure the system against insider threats.

Regarding the problems I referred to above, one related to the results. Op Bravo had announced that the paper and electronic records produced the same results, but their press release made no mention of discrepancies later uncovered by University of Miami Law Professor Martha Mahoney: Voter Certificates attesting to eligibility were signed by 95 people, but only 93 ballots were cast, and only 92 Voter Choice Records were included in the audit.[footnote: Martha R. Mahoney, "Comment on Pilot Project Testing and Certification," EAC website, April 2010, http://www.eac.gov/assets/1/AssetManager/Martha%20Mahoney%20-%20Comment%20on%20Pilot%20Project%20Testing%20and%20Certification.pdf]. Part of the explanation, as mentioned on the Operation Bravo website, is probably that a voter interrupted the voting process, and did not try a second time. However, no incident report was prepared, so we can only guess at the cause of the discrepancy.

I also suggest that you change Finding 8 to read as follows:

"Finding 8: Although all voting methods must be monitored carefully to prevent malicious or negligent event, remote digital voting, especially the digital return of voted electronic ballots with no audited paper ballots, is far too insecure to be used for the foreseeable future."

Yours

Barbara Simons, Ph.D.