At the May 5, 2004 hearing, Vice Chair Gracia Hillman of the Election Assistance Commission asked the technology panelists to submit the answers to a question. Here is my answer, along with a few comments on other issues that came up in the hearing.

The question came up about lever machines, and the difference between voter verifiability of lever machines versus DREs. In general, I believe that lever machines share a serious problem with DREs in that they are not voter verifiable. I have always been an opponent of lever machines for this reason. However, I also believe that there are two additional disadvantages of fully electronic DREs that are not shared by lever machines. The first is that if someone tampers with a lever machine and it is opened up for inspection, the tampering will be evident. That is not necessarily true of a fully electronic system, where tampering can be with data stored on magnetic media. The other principle difference is that to rig an election with lever machines, someone would have to tamper with many, many machines. Whereas if someone were to rig the software in DREs to fix the outcome of an election, they would only have to do it once, and the malicious code would exist in many, many machines. It is easier to scale the tampering if it is done in the software that is preinstalled on the machines. Finally, I should note that the fact that lever machines are not voter verifiable should not be used an excuse to produce electronic voting equipment that is also not verifiable. Rather, we should strive for constantly improving the state of the art, and not substitute a terrible technology for a bad technology.

There was one issue that came up during the election officials panel that requires a response. One of the panelists suggested that the DRE machines can print a ballot image of every ballot that was voted on the machine, and that these could be counted. It is important to note that from a security perspective, this recount is meaningless. If a DRE is rigged so that it provides the wrong result at the end of the election, it can just as easily be programmed to print ballot images that add up to the same incorrect totals. This is why the phrase *voter verifiable* is so important. Today's most popular DREs can print ballot images, but that is nothing more than a marketing gimmick. Those printed ballots can be recounted, but that is an exercise in futility if the machine has been rigged or tampered with. Only by counting ballots that the voters acknowledged were correct can we hope to achieve something by recounting.

Aviel D. Rubin
Professor, Computer Science
Technical Director, Information Security Institute
Johns Hopkins University