PUBLIC HEARING

STATE OF CALIFORNIA

SECRETARY OF STATE

SECRETARY OF STATE'S OFFICE

1500 11TH STREET

FIRST FLOOR AUDITORIUM

SACRAMENTO, CALIFORNIA

MONDAY, NOVEMBER 26, 2007

10:04 A.M.

JAMES F. PETERS, CSR, RPR
CERTIFIED SHORTHAND REPORTER
LICENSE NUMBER 10063

PETERS SHORTHAND REPORTING CORPORATION (916) 362-2345

APPEARANCES

PANEL MEMBERS

Mr. Tony Miller, Moderator, Chief, Political Reform Division

Ms. Judith Carlson, Elections Divison Counsel

Mr. Lowell Finley, Deputy Secretary, Voting Systems Policies

Mr. Lee Kercher, Chief, Information Technology Division

Mr. Bruce McDannold, Interim Director, Office of Voting Systems Technology Assessment

Mr. Chris Reynolds, Deputy Secretary, HAVA Activities

ALSO PRESENT

Dr. Judy Alter, ProtectCaliforniaBallots.org

Ms. Judy Bertelsen

Ms. Kathay Feng, California Common Cause

Mr. Steven V. Freeman, Freeman, Craft, McGregor Group

Ms. Michelle Gabriel, Voting Rights Task Force

Ms. Jennifer Kidder, Voting Rights Task Force

Mr. Dean Logan, Los Angeles County Registrar of Voters

Mr. Chris Ortiz, Unisyn Voting Solutions

Mr. Jim Soper, CountedAsCast.com

Ms. Ann West

INDEX

PROCEEDINGS

MODERATOR MILLER: Good morning. Good morning. Can you hear me? Yes. On the record.

Thank you for participating in today's proceedings. You know the drill. Please silence any cell phones or pagers, including me.

My name is Tony Miller. I'm Chief of the Political Reform Division of the Secretary of State's Office. And I'll be moderating today's proceedings.

This public hearing is designed to receive input regarding the InkaVote Plus Voting System that is manufactured by Election Systems and Software, or ES&S -- I will refer to the vendor as ES&S -- and as used in Los Angeles County.

This system was reviewed as part of the Secretary of State's top-to-bottom review of voting systems used here in California. The reviews of three other systems were completed in July. But because ES&S was late in delivering their equipment to the Secretary of State's Office for review, the InkaVote Plus system was decertified on August 3rd, 2007, pending a review by the Secretary of State.

Before we begin, let me take a moment to lay out the guidelines under which today's hearing will operate.

This is a public hearing. It's being transcribed

and videotaped, meaning that all oral comments made here today and written comments that are provided become a matter of public record.

The flickering of the lights is an issue with which we're trying to deal. We hope that that's short-lived.

This is a public hearing. This is not a public debate. I know this is an issue about which people feel very passionately.

The audio system is also challenged. One moment please. This seems to be working. I apologize.

However, it is essential that you respect the rights of others to express their opinions and public comments, even if you disagree with them, even if you feel the speakers are wrong.

In any case, booing, hissing, applauding, shouting, jumping up and down, sign waving, or other displays of support or opposition are not acceptable and will not be tolerated. And I will not hesitate to ask that people who cannot abide by these very simple requests for common courtesy be removed from the auditorium.

Conduct that will not be tolerated includes audible communications with your neighbor during the hearing. Pass notes instead of talking if you must communicate, please.

If you would like time to speak during the public comment session of the hearing, you must fill out a speaker's request card. They're available at the desk out in front of the auditorium and from staff. If you need a card, let me know and I'll make sure that you've received one.

This is a public hearing where the researchers who examined the InkaVote Plus system will publicly deliver a report on research that they conducted on behalf of the Secretary of State's Office.

The goals of this hearing are as follows:

To have the report publicly presented. A copy -- the Red Team report is posted on the Internet on the website of the Secretary of State's Elections Division under Voting Systems.

Also, to give ES&S and the public an opportunity to comment on the report.

And, thirdly, to collect information from ES&S and the public that may help inform the Secretary of State's decision about what, if any, action to take in the wake of this report.

The panelists here today won't be voting or deciding whether to adopt the report, nor will they be commenting on the report's findings or expressing opinions on what the Secretary of State may or may not do or should

do as a result of this report. Rather, the panel is here today to formally receive the verbal report from the research team, to receive comments from ES&S and the public relative to the voting system and the report, and to bring a variety of perspectives to the issues raised in the report and by all of you when it comes time to sit down with the Secretary of State to review and analyze all of the information that has been collected, and to take appropriate action.

The panel members are, seated to my immediate right, Lowell Finley, Deputy Secretary of State for Voting Systems Policy and Technology; Judith Carlson, Elections Division Counsel for the Office of the Secretary of State; Bruce Mc Dannold, Interim Director of the Office of Voting System Technology Assessment for the Secretary of State's office; Chris Reynolds, Deputy Secretary of State for HAVA Activities; and Lee Kercher, the Chief of the Information Technology Division for the Office of the Secretary of State.

Delivering the report today will be Mr. Steve Freeman, a partner with Freeman, Craft & McGregor Group, that was hired to study the ES&S InkaVote Plus system.

I would now like to call upon Mr. Freeman.

That should be working.

Technology assistance. Mike.

MR. FREEMAN: All right. Before I start I'd like to mention my ears are blocked up. I'm not sure exactly how loudly I'm talking.

MODERATOR MILLER: You have to get close to the mike in order for it to operate.

MR. FREEMAN: Okay. Yeah, that's better.

As I said, my ears are blocked up. I'm not sure how loud I'm talking or how much this microphone's going to help. If there is a problem, please hold your hands up or let me know so that I can go ahead and repeat.

FCMG was asked to conduct and manage the testing for the security reviews both for the Source Code Review and the Red Team penetration attack. FCMG itself does not have sufficient expertise in these areas and we are contracting with the firms and organizations that do have for such tests.

In this particular case we contracted with Atsec information security out of Austin. Atsec is a recognized and accredited cryptology module testing laboratory and common criteria laboratory. They use some of these skills and experience in performing the testing. And we actually took advantage of the common criteria to go ahead and provide a more useful report in terms of the results in the form of vulnerability assessment.

The particular system that were under test is the

InkaVote Plus system. It's marketed by the Elections Systems & Software, ES&S. It consists of the InkaVote Precinct Ballot Counter that is produced -- actually manufactured by the International Lottery & Totalizator Systems, Incorporated, and the Unisyn Election Management System software, sometimes called EMS.

The PBS is based on a stand-alone lottery ticket machine. And the system supports the InkaVote ballot, which was not developed for this system. It was based on the ballot that has been used in Los Angeles for several years.

The InkaVote ballot is a mark sense ballot based on the design of a Hollerith punch card. Ballot identification data is pre-punched in the leading columns. To vote, the card is placed in a marketing device which has a ballot voting booklet and template guide showing the location to mark a vote for each candidate in each contest. A special marketing pen is used to mark the voter's choices.

The InkaVote Plus PBC unit is also equipped with an additional component called the Audio Ballot unit which provides support to assist visually blind as well as other voters who need an audio ballot.

The Audio Ballot unit consists of a keyboard, earphones, and printer, but has no visual screen to review

the content of the ballots.

The unit uses the audio ballot script which guides the voter through voting their choices and prints a marked InkaVote ballot. The voter may then insert the marked ballot into a PBC unit which checks for overvotes and blank votes. Other voters who mark their ballots manually or with the ballot booklet template may also use the PBC unit to check the ballots for overvotes and blank ballots. This overvote and blank ballot feature is a part of the requirements originating in the Help America Vote Act.

Although the PBC unit's capable of tallying the ballots and producing a machine report of the results when the polls close, the City of Los Angeles and County of Los Angeles only use the system for the audio ballot and the error checking functions without using the ballot tally or reporting functions. The InkaVote ballots themselves are taken to a central site and counted on the existing machines for their central count operations.

The Unisyn EMS suite of applications is a set of Java-based software applications which allows the user to create election definitions for the PBC, load the election definitions from one or more PBCs using Ethernet Link. The suite also includes the option of load compatible XML formatted election definitions from other election

management systems. Once the polls close, the tally results may be transferred back to the EMS suite for accumulation of multiple PBC results and reporting. The Unisys EMS suite of applications operates on a Windows XP-supported workstations. The EMS component applications operate independently and may be installed on separate workstations as needed. They include:

An election database using MySQL;

The application to modified and define the elections;

The Election Converter, which converts an XML description of the election, produces an encrypted Election CD;

The Election Loader, which actually loads the definitions -- election definitions from the Election CD into each PBS;

A Vote Converter to transfer the voting results from the PBC using a USB memory device;

And the Vote Tabulation module itself.

Under the usage within L.A. only the Election Converter and Election Loader are actually used. In terms of the focus and the scope of the testing, Atsec was asked to focus and concentrate on those particular modules and functions. However, they were provided a full suite of software and a full technical data package for review.

They were not expected to necessarily search through those for the additional functionality. But they were permitted and encouraged to go ahead and take a look at those sections if necessary to complete the analysis for the operations.

The entire Red Team actually used the features to go ahead and produce some vote results on some of their tests and exploits that they used to show the performance of those exploits.

The particular tasking under the notations with Los Angeles County was to detect and prevent the casting of ballots, which was the -- with the specific purposes of detecting and preventing casting of ballots which were blank, detecting and preventing the casting of ballots which have at least one overvoted race, or to provide the Audio Ballot interface which marks the ballots for voters requiring the audio ballot.

For the particular review for vulnerabilities, Atsec was asked to particularly look at the integrity of the election definition needed to support the error detecting and Audio Ballot functions; to review for issues of vulnerabilities involved with the tampering or altering of the security audit logs and the log reporting services; and the basic operations of the PBC in the form of denial of service attacks.

For the purposes of the test, the test team was asked to consider four classes of attackers:

A voter: Which usually has a low knowledge of the voting system machine design and configuration, and very limited in terms of time access to the machine itself. As recognized, the voter may be carrying out attacks designed by others or carrying materials developed by others.

Poll worker: Usually has a low knowledge of the voting machine design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others. They have access to machine for less than one day in a public venue.

The election official insider: Has a wide range of knowledge of the voting machine designs and configurations. They may have a restricted access for long periods of time. Their designated activities include the set up and the pre-election procedures, election operation, post-election process and results, and archiving and storage operations.

Atsec recommended the addition of one extra category, the storage worker, which basically is involved in the set up and pre-election procedures and the archive and storage operations.

And, finally, the vendor, who has great a great

knowledge of the voting system design and configuration. They have unlimited access to the machine before it is delivered to the purchaser and, therefore, may have unrestricted access while performing warranty and maintenance services and when providing election administration services.

The team was not limited to these attackers, and their directions included direction from Resolution 1705 of the Technical Guidelines Development Committee of the U.S. Election Assistance Commission, adopted at the TGDC plenary meeting on January 18th and 19th of 2005, which basically calls to recognize the attacker's vulnerabilities should not exclude those involved in collusion between multiple parties, including the vendor insiders, and should not exclude those involved in adversaries with significant financial and technical resources.

Excuse me a second.

More specific tasking, directing some of the items and issues in particular that they were supposed to look for and report on. The emphasis was on security and integrity of the system. In particular:

The adherence to the applicable standards in sections 4, Volume I (software standards), 7 of Volume I (quality assurance), and 5 (software testing) of Volume II

of the 2002 Voluntary Voting System Standards.

Adherence to other applicable coding format conventions including best practices for the coding language used, an any other standards identified through IEEE, NIST, ISO, or NSA standards or guidelines which the reviewers find reasonable to apply.

Analysis of the program logic and branching structures.

Search for exposures to commonly exploited vulnerabilities, such as buffer overflows, integer overflow, inappropriate casting or arithmetic.

Evaluation of the use and correct implementation of cryptographic keys and management.

Analysis of error and exception handling.

Evaluation of the likelihood of security failures being detected. In particular: Are audit mechanisms reliable and tamper resistant? Is data that might be subject to tampering properly validated and authenticated?

Evaluation of the risk that a user can escalate his or her capabilities beyond those which are authorized.

Evaluation of whether the design and implementation follow sound, generally accepted engineering practices, including whether the code is defensively written against bad data, errors in other modules, changes in environment, user errors, and other

adverse conditions.

Evaluation of whether the system is designed in a way that allows meaningful analysis.

Search for embedded, exploitable code such as "Easter eggs," that can be triggered to affect the system.

Search for dynamic memory access feature which would permit the replacement of certified executable code or control data or insertion of exploitable code or data.

Search for use of run-time scripts, instructions, and other control data that can affect the operation of security relevant functions or the integrity of the data.

The review was conducted at the 2nd and 14th of October at the Atsec office in Austin, Texas. The team consisted of two experts from Atsec and was supported by meetings from FCMG.

My understanding, there's been an observation that we did not actually identify the individuals. And I propose that we make an amendment change to the report to reflect that the individuals involved was Klaus Weidner of Atsec and Stephan Muller of Atsec.

The documentation review examined the ES&S Technical Data Package and the source code. The TDP and source code were copies of the TDP and source code that was used by the NASED Independent Test Authority lab in its original federal certification.

The integrity of the delivered documents was verified from electronic file signature hashes provided by FCMG from the trusted sources original disks.

Atsec divided the documentation review into two categories for reporting: The sufficiency to enable review of source code; and the sufficiency to design and conduct tests.

And I'll be going through detail on that and the individual categories that was identified for the Source Code Review.

The Source Code Review used a combination of manual review and automated data collection and analysis methodologies to identify potential areas for exploitation.

Because of the limited time of 12 days and its broad scope, including both document review and source code review, the team concentrated on surveying a breadth of categories of vulnerabilities that they could identify, and only reviewed in depth enough samples of each of the categories to determine how that vulnerability was being handled. No attempt was made for all the categories to enumerate how many instances existed. Other Source Code Review projects is likely to find more, but those findings should be within the listed categories.

Test tools included lexical scanners and special

code review tools from open sources, commercially available search and analysis tools, and numerous developed scripts.

The details on where those tools are and what they are are confined -- or within the confidential reports this time because there were felt they too much for a guideline on how to go ahead and actually carry out some of the identified exploits.

I will mention --

PANEL MEMBER FINLEY: Excuse me, Mr. Freeman.

If you could go just a little bit slower. I think your rate is probably starting to catch up with the court reporter, who has to get everything down.

MR. FREEMAN: Sorry.

PANEL MEMBER FINLEY: We can follow you just fine. But he's got to transcribe it.

Thank you very much.

MR. FREEMAN: I should mention in the confidential reports are very explicit descriptions of the actual attacks and exploits that were developed, including actual scripts, codes, modifications of the tools to actually break into the PBC and other uses.

For this reason, I believe that they're going to be kept confidential to avoid these being just an open door opportunity for someone to go ahead and exploit the

system using this information at this time.

Okay. Going through the individual sections.

In reviewing the document assessment, the sufficiency to enable review of source code. The review consisted of a review of the vendor's system design specifications and usage procedures. They found there was no detailed description of the source -- software components and algorithms that could be directly compared to specific software modules in the source code. The documents were very limited value to conduct a deep assessment which allows searching for vulnerabilities.

Within the report is a summary table of the different findings. This particular finding is listed under A.1. There's no specific vulnerabilities identified because of a lack of information, so there's no vulnerability assessment for this particular finding.

The sufficiency to design and conduct tests. The system test and verification plan does not contain any test procedure description. It only provides a very abstract description of areas to be tested. The provided documentation does not show evidence of conducting tests at every level of the software structure. The TDP and source code did not contain unit tests or any evidence that modules were developed in such a way that program components were tested in isolation. This doesn't mean

that this wasn't particularly done. It's just we have no record or evidence of it.

Summary table Item A.2 examined a specific section of the documentation specified in some of the encryption for communication. This case did have a brief explanation on how some cases were being implemented, but they're not specified where. The description was inconsistent with standard practices in a referenced encryption practice and represented a serious form of -- vulnerability. But they were unable to identify where it was used to apply it from the Source Code Review Team.

In actual fact, the Red Team in penetration managed to go ahead and exploit some of this functionality, and did so without particular reference to the source code team at the time.

Summary table Item A.3 provides another specific documentation review case, with a subject of Linux hardening. For the benefit of people who don't understand this particular jargon phrase of "hardening," that's a practice that's come into vogue, and it's being defined under released published guidelines and standards, first was started by Microsoft in terms of their operating systems recommend how their default installation can be modified to provide more secure operation.

NIST, NSA, and some other organizations got into

provide further guidelines and detailed checklists. And currently revised checklists are being published by the -- I believe it's the Center for Internet Security.

The documents reviewed are the configuration of management plan and system security specification, system functionality, and system configuration review of the PBC. They found inconsistencies, wrong references, and the lack of technical details on the actual hardening procedures to recommend it to being used.

Based on the level and the lack of reliable information, the Source Code Review Team could not assess the quality of hardening. However, the Red Team did report in their test, encountering some good hardening practices on the test machines that prevented many common attacks. But these were apparently done by the ES&S and ILTS installation crew to set the system up for Red Team testing and may not be documented.

The Source Code Review Team did note that the versions of the Linux Operating System described as an older version is not being maintained. This means as new vulnerabilities are detected for those particular versions, there is no attempt to create security patches or address how those vulnerabilities can be stopped. The Red Team was successful in several attacks using openly known vulnerabilities on this basis.

The vulnerability assessment on that particular report item was labeled as "basic," which is the lowest, weakest -- or I should say the most vulnerable category that is listed.

Summary Table A.4, on the Configuration Management Plan -- Item A.4 on the Configuration Management Plan specifically. The Review Team for on the plan provided all the steps within the development cycle and was generally a fairly reasonable document.

However, the system security specification identified the files being generated as part of the configuration process for the customer.

The Red Team had found the file and determined it contained the jurisdiction key, determined it was used to create encryption keys for the election, and used it plus some other information to open all the files, including the supported encrypted files in the Election CD. The problem that the Review Team identified was that there was no description of how or when the file was created and how it was handled, how it's updated, or how it was distributed. As it is a significant factor in the creation of the encryption keys used by EMS and the PBC, the secure handling and management is necessary but undocumented.

No assessment was made on this item within the

Source Code Review because the basic confidentiality of this key is not known. We don't know how it's protected, how it's treated, to try to prevent this exploitation to be used.

Next is the source code assessments. I'm not going to go into detail through it. I'm just going to try to summarize very briefly. But there's a detailed listing within the public report.

The first item was the adherence to applicable standards, including the voluntary -- excuse me -- the Voting Systems Standards of 2002. Volume 2, section 5.41, which is controls and constructs. Basically it just noted that the Java supports all those particular control instructions, and there was no incidents identifiable that violated those.

We also checked for the quoting conventions, under 5.42 of the same document. There's a number of items, about 25 of them, that's listed there.

For the most part, most of the incidents that are found within this are relatively minor infractions that are acceptable in practice. There are a few that indicated some potential other problems.

Probably the main one had to do with -- identified under Uniform Calling Sequences and a couple of the others, that there is a -- does not seem to be any

parameter -- input parameter check nor validation. The system assumes that any inputter as being passed to a particular method under the Java is correct and contains no errors. There's a number of potential exploits that could be made advantage of this. And there was described in some detail some specific examples.

Functional returns under Java -- this is not really a big issue -- where they did notice, and this is another problem that shows up, more in terms of the documentation than necessarily actual implementation, but there's a considerable use of exception handling under Java to go ahead and do abnormal exits.

There's some cases within those that there's exception handing. It is not clear on how controlled, the test, or why it's been treated as abnormal. This is considered important in an improper and a poor style. It doesn't allow for accountability and review in those particular conditions.

It's not -- it does not look like any of these were a particular problem, the current versions. But this is a potential method to hide different types of attack.

Vote counter overflow. The principles in the voting system standards identify that it should not depend on the expectation that the counter value was too large to cause an overflow. Potential problems in terms of

malicious code changes, memory failures, and other sources can result in those values being exceedingly high. So the recommendation is that there is very positive steps to check to make sure that the values are not growing uncontrolled and out of bounds. There is no attempt to check the vote counter overflow.

Those particular counters under the nature and the design under Java are very flexible and very likely not to overflow. But this doesn't take care of the additional conditions that may occur.

Lines containing multiple statements. This is an issue because the introduction of the lines containing multiple statements under -- are not necessarily determinable. That is, under one operation they will work one way and in another they may work it different. There was only two incidents of lines containing conditional and executable statements. And these were considered basically acceptable.

Identification of constants other than 0 and 1. This is a coding style issue mainly for the maintenance code and recognizing what's going on with the code. The standards originally had these requirements that such constants were to be defined in some way so they could tell what the basis of the range of values and how they're appropriately used. There were similar various examples

where they may have replaced the constants with some sort of variable, but the variable name itself contained no additional information. For example, the number 4 was replaced by the variable 4. It does not tell how this is being used, what's the purpose for it, and what the basis of the range may be involved.

Conditional "?:" operator, especially when multiple call is necessary. One case was found. This is not considered to be a real serious risk or problem.

Again, this a condition that can result in implementation errors under different compilers and situations. It's more controlled under Java than it is under some of the other languages that uses it.

They also reviewed against adherence to other standards. And the developer did not specify or indicate any specific additional coding dimensions. Specific cases of instructions in source code which are inconsistent with best practices are indicated there's appropriate places elsewhere in the report.

The review program logic branch instructions. Again, this was addressed under many other topics.

Commonly exploited vulnerabilities, such as buffer overflow. This particular case Java provides its own protection against the buffer overflow explicit attack method.

The integer overflow. We've already mentioned it.

Inappropriate casting or arithmetic. No obvious instances of such conversions were found.

Cryptographic and key management. It was actually multiple potential and actual vulnerabilities. This is probably the most serious problem that was found.

The cryptographic algorithms use a symmetric cryptography only, which introduces vulnerabilities as noted in the summary table.

And the master key algorithm is a very weak home root cipher, also noted under some of the specific test cases and documented. In that particular case they found instructions on how to break it under Wikipedia.

The key management. The cryptographic key management is basic symmetry keys, which introduces vulnerabilities. Because these particular keys are used both for the encryption, decryption, and validation, with those keys available it's possible to go ahead and replace the election definition, for example. And this exploit was demonstrated with the false election definitions using the same keys so the system validation did not identify or catch the change.

In addition, there was issues in terms of the key management. One of the critical keys, the jurisdiction

key, was discovered in a file that had the critical portion of the text of the key in clear text. The Red Team was actually able to take this without additional information from the Source Code Review and break down most of the inscription included in the system to open up the Election Definition CD, identify additional keys and encryption codes are being used, and to replace the Election CD with another one that carried out further exploits and attacks.

Hash check the integrity. They're only using hash checking, sometimes known as file signatures, to check, make sure there's not an accidental corruption of the file. But the implementation on it is insufficient to cash deliver tampering, because the check version of the hash totals, the values that are going to be checked against what's generated, are actually embedded and buried within the file. And then if the file was actually changed, the attacker could easily change that hash value to match what was there. And this was demonstrated in one of the exploits involving the Election CD.

Error exception handling. Exception handling under this was heavily used. There was 272 incidents were found to bypass normal control flow. Under Java this is not necessarily a bad condition. It's recognized in cases where there is a particular condition that could cause

damage to the system. Rather than allow it to carry through, it's sometimes appropriate to go ahead and catch it and handle it and treat it in the appropriate manner, either to halt the system for an item that is not likely to occur during the operations, or to provide some sort of correction or adjustment so the integrity of the system would be preserved.

Most of these is deemed acceptable uses basically involved in the stopping conditions before the errors cause damage -- consider as acceptable, represent conditions that were not abnormal conditions.

These again, as I mentioned before, can be potential exploits, like a Trojan horse or another attempt to identify using that exception condition to trigger off some sort of malicious attack.

The particular incidences found were not harmful in their form. It was just considered a basically bad practice supporting the possible introduction of viruses or other malicious software.

The likelihood of security failures being detected. There's a basic lack of privileged separation and design that does not support reliable detection issues and security features -- figures. Excuse me.

Basically this had to do with a reliable and tamper-resistent audit. Design documents and code

comments do not provide any evidence that audit logs are protected from tampering. The code statements being logged have sufficient privileges to modify or delete logs. The design documentation did not mention the use of operating system futures that support the integrity of the logs. This doesn't say that some of those features not being -- were not there, but they were not found and they were not identified in the documentation.

This also ties into the next item, privilege escalation. This is where someone can go in and gain privileges that they would not ever have -- they'd be restricted -- bypassing some of the controls such as gaining privilege to go ahead and change, add new users, and changing the security settings and parameters that are supposed to be protecting the system.

Unfortunately, this particular item was not considered applicable because all the applications run at the top level of priority.

This is a -- issue, as software engineer and security principle, of which principle is not being exercised.

Going into best practices and defensive coding, which were -- most of the vulnerabilities were found. Although most of them are extensions on the items already identified.

Run-time construction of SQL statements. There was 116 incidents of SQL statements embedded in the code, with no evidence of sanitation of the data before we started the SQL statement. That is, there was no check verification against the information on the SQL statement to see that it was acceptable statement to be used at that particular time.

Best practices say that for run-time SQL statements, if they're going to be used at all, generally they're considered a bad practice. But if they are going to be used is to use pre-defined hard-coded SQL statements using bound variables. They're identified and checked to make sure that the variables were within acceptable limits.

In particular, there was identifiable vulnerabilities found and documented in the vulnerabilities assessment, A.10, under what's called the SQL injection, a very serious form of attack. These injections was demonstrated to go ahead and be used to actually go into the database change values, parameters, and structural election definition.

An item called the Zip File Directory Traversal. It's documented in A.9. This particular one goes ahead and acts as a zip file to get some information. They found that it permitted the use of basically as patterns

identifies his path name. And his path name could be changed so that the files that were loaded, opened up, extracted under this would actually -- to overwrite other files within the system.

For the ad hoc conversion of two-digit year values, they had minor program errors. There was a limited range of years in which it would work correctly. And there was some other issues with this. General practice errors if they both store two-digit year values, we're going back to living with a Y2K thing. They should be stored as four-digit values. These were identified basically as minor coding errors, but they probably need to be taking care of.

System amenability to analysis. This is not so much of a looking for vulnerabilities, but to see whether you can even review and find vulnerabilities within the system documentation.

Lack of design documentation, appropriate levels of detail. It was observed that some of the documentation, barely stated, the system had the qualified requirements without giving specifications of how.

The design does not use privileged separation. We've already mentioned that one.

There's unhelpful or misleading comments in the code, that basically state something different than what

has actually happened.

There's a potential complex data flow due to the extensive exceptional handling, rather than using the normal control flow methods.

There's a large amount of source code compared to the functionality implemented. There's much simpler pre-defined functions and values that could be used for some of these functions.

There was no examples of supporting the code of "Easter eggs".

There is no inserted back doors, Trojan horses. However the zip file directory traversal problem and the SQL injection at a run-time level could be exploited as a back door.

Dynamic memory access features. Basically the Java protects against these approaches.

Run-time scripts and instructions and control data. This is where something's available that you'd go ahead and change the actual program control and function during run time. Usually we're looking for things like interpreters or control programs that are fed particular scripts. In this particular case the SQL interjection problem is a type of section problem to some extent; and particularly in terms of a threat against the election definition file. The had an election definition file that

sort of provides control data. And the demonstrated attack where they modified or changed the Election CD without being detected is an example of this type of attack.

As a mission there's a table that breaks down each of the identified vulnerabilities plus three of the items involved in the documentation -- actually four. Three of the items in the documentation regarding level of information was available did not really identify vulnerabilities could be assessed. So they're listed as non-applicable. The rest of them were accessed. They were basically list -- all of them were considered basic, the lowest level, except for one, which is considered enhanced.

Factors to make up those particular evaluations include the time of access -- the amount of time to be able to access the equipment or the software. That may not be necessarily in a spot. That could be a case where the software or information is captured by someone, let's say, a co-worker, you know, taken off line to be developed further over a longer period of time.

The expertise of the attacker in terms of general knowledge about the particular type of operating system, features, a structure, encryption, so on.

The knowledge of the actual system itself,

particular details about the system that may be involved in some of the more confidential particular data package around a source code.

Window of opportunity. This is closely related to the time that this talks about just how much access -- how close the time is that's available to access this particular feature or capture this particular information.

And the type of equipment, whether special tools are needed. For the source code purposes, it's interesting to note that there was no special equipment that was required at all. For the Red Team attack they did use some minor special equipment in terms of special software tools. But basically most of this could be done with common office information or features utilities within the operating systems themselves.

This vulnerability assessment needs to be approached carefully. This identifies the particular vulnerability in terms of uncontrolled access to the equipment, the device. No more practice under good -- voter system security practices developed over years requires a tighter control, physical security and procedurally. Many of these particular attacks may be ameliorated by those procedures, but this was not part of the Source Code Review. And these particular vulnerabilities need to be assessed against those

procedures. However, they do vary greatly between different jurisdictions. Some small jurisdictions may not use any particular ones because they have direct control by one or two individuals. Other larger jurisdictions may have very complex procedures, and in the process may be more vulnerable in other ways.

Even those may be judged that they're acceptable risk given the local procedures, many of these are recommended that they be corrected anyway in case of those procedures lapse more fully in some fashion.

I'm now going to go on to the Red Team attack.

The Red Team attack basically has some information -- they didn't take as full advantage of the TDP, they didn't go through a particular assessment of it. It was conducted in about five days. There were three people involved. Atsec had two. There was Lewis Lucy and then Steven Weingart. FCMG also had an employee there, Jack Stauffer, was involved in the top-to-bottom reviews that were done, some were on other systems, and has extensive knowledge of working in terms of penetration testing.

They had five days to conduct the test, 2-7 October, in the secure testing facilities in the California Secretary of State's offices.

The testing began with the introduction and setup

by ES&S and ILTS who were to configure the system in a recommended hardened condition for operation and prepared a test election for use in the testing.

Based on the initial exposure to the system and the industry standard knowledge that errors typically occur at system interfaces, an initial penetration plan was generated which focused on:

Physical security of the Polling Ballot Counter, the PBC, of the InkaVote Plus system.

Physical security of the ballot box attached to the PBC at the polling station.

Contents of the Election CD created by the election generation sub-system of the EMS program.

Logical security of the files and configuration of the system unit contained within the PBC.

I just noticed an error on that previous one. That should have been Election Conversion system.

The logical security of the files and configuration of the system unit contained within the PBC.

Logical security of the programs used and the files generated by the EMS program, the Election Loader, and the voting Tabulator.

Security of the networking methodologies used to communicate the election data by the Election Loader to the PBC.

The penetration testing used a combination of manual and automated data collection and analysis methodologies to identify potential areas for exploitation and exercised some samples of that exploitation.

Testing included but was not necessarily limited to:

Examination of top-level system design and architecture and the examination of system documents and procedures which was done by the Source Code Review Team.

The examination and open-ended testing of relevant software and operating system configurations.

Examination and open-ended testing of hardware, including examination of unused hardware ports and security measures to lock/seal hardware ports used.

Examination and open-ended testing of system communications, including encryption of data, and protocols and procedures for access authorization.

Test tools used included common household and office equipment and chemicals and a number of software Unix utilities, password crackers, and penetration tools that are readily available over the Internet. Again, specific sources were listed in the confidential report.

I'm not going to go in quite as full detail as I did in the Source Code Review.

Their attack was very, very straightforward, very

business like. They approached -- actually they split up. They had one of the persons conducting the physical attack with assistance from Jack Stauffer, and the other one performed the technical attack against the operating systems that were installed in the software applications. And they both worked in terms of dealing with the communication of the transfer of information between the different components.

And the physical access for the PBC. The PBC unit consists of a top half, which we'll call the PBC head, containing a computer system, ballot scanner, printer, and touch screen display for the use of the poll worker, and a connection for the Audio Ballot unit. The bottom half is the ballot box. The election configuration is stored on the computer's hard disk and is used to manage the scanner, printer, and the Audio Ballot unit, to process ballots for the election.

A transfer device, which is a USB memory device such as full drive, may be connected to a USB port housed behind a door on the a left side of the side of the PBC that faces the poll worker. The transfer device is used to transfer the election data from the PBC to the Election Management System via the Vote Converter. Although transfer of results was not included in the limited scope of this study -- because of its use in L.A.; the L.A.

doesn't use that -- the port and the transportation device were considered as potential access points within the examination. And an actual attack was identified using their port.

In transportation of the PBC from storage to the polling place, recognizing normally the PBC is programmed at the warehouse and then taken and exported to the polling place, additional security is provided by a lid that's screwed down. In this particular case, the user documentation does not specify the use of any tamper-proof seals or other methods to detect if the lid or the PBC has been tampered with during storage or transportation. And this is identified within the Red Team's report as item A.1 among the vulnerabilities.

In the physical security testing, the tamper-proof seals, including both paper seals and plastic, were easily removed without damage to the seals using simple household chemicals and tools that could be replaced -- and then the seals could be replaced without detection. The tamper-proof seals were actually well designed where it would show evidence of removal. And if they were simply peeled away, they would show up as being void. They were a fairly good quality of seals. But the housing is such as it doesn't form a good enough bond and simple household solvents can be used to remove the seal

unharmed. And then the seal could be replaced later without detection.

Once the seals were passed, simple tools or easy modifications sills to simple tools could be used to access the computer and its components. It took less than 20 minutes to open up the case and remove particular components and replaced by devices or equipment that would go ahead and be used to perform other attacks.

The key lock for the transfer device, which uses a special key that's supposed to be secure, could be unlocked using a common office item -- I'm not going to name how it is, that should not be that easy to do -- without the special key. And with the seal removed, he had full access to the USB port.

The USB port itself may be used to attach a USB memory device, of which contains an alternate operating system, and used to gain control of the system and to be able to access the files and change the files within the computer itself.

The keyboard connector for the Audio Ballot unit was used to attach a standard keyboard, which was then used to gain access to the operating system using alternate methods to sign on. So in the cases where the hardening probably could be improved, at some benefit, without even opening the computer.

In combination these two provided full access to everything in the system and the ability to change and modify.

Note that there's no method to determine if the box had been opened in transportation, which is an issue that sometimes can occur with a practice that I've heard called sleepover. This means that this system could be changed extensively before this is being used with an election. The one problem with that would be if the procedures provide some sort of authentication check followed afterwards. But, again, use of the hash and checks, verification and validation, and some of the other features were found to be vulnerable to go ahead on modification to avoid these particular detection methods.

The seal used to secure the PBC head to the ballot box for transportation -- oh, excuse me -- during actual operation provided some protection. But the actual user manual, the InkaVote Plus Manual UDEL, provides instruction for installing the seal that, if followed, would allow the seal to be opened without breaking it.

Essentially the instructions actually demonstrate putting it in -- attaching it in backwards.

Even if the seals were attached correctly, we found there was enough play and movement in the housing that it was possible to lift the PBC head unit out of the

way and insert or remove ballots.

In actual fact, removing ballots was very tricky. I'm not sure this really would qualify as a significant attack, because in this particular case the PBC is set up and operational within the polling place. The poll worker sits behind it and has it under constant observation. Other poll workers can see it; at least they should under good operations practices. It would be difficult to believe that this could be done. If there is collaboration enough to allow this to occur, there's probably far more serious problems within that jurisdiction than is necessarily being treated by making the technical corrections or changes. However, in spite of that, this particular problem should be corrected.

The PBS logical system access. This is gaining a system to the actual operation system or the code. Attempts to log in with invalid passwords were unsuccessful. But they revealed error messages that actually provided information about the passwords that could be used to reduce the effort for an exhaustive attack. This is something that not probably could be happening in a single day. But if there's not good security protection against these passwords to change them out frequently and as necessary, this exploitation could become very serious.

After the physical box was opened, other methods of gaining access were tried and either succeeded or revealed enough to show the other attacks were feasible. This is reported under the A.10 item within the work papers and description of the actual vulnerabilities. Very specific details. The summary table for one method.

Making changes in the BIOS to reconfigure the boot sequence allows the system to be booted up using external memory devices containing a bootable Linux copy. This is in A.11. Examples against this are replacement of the actual hard drive on the system, attachment of additional hard drive, or attachment of a USB memory device to the USB port.

Once done, all of the files can then be accessed or potentially modified, including sensitive files such as the password file, which are known to be -- they can be opened and cracked by an openly available and well known cracker programs on the Internet.

Also, new users could be added with known password. The system's resealed, closed up. And those new users can gain access to the system during operations and make any such changes as they need.

On the EMS and Election Voter System. The EMS workstations were secured with non-trivial passwords following recommended minimum guidelines. This was a good

operation. The EMS workstation as installed for testing were configured with most non-essential services to say we're part of a hardening. But other hardening steps were not used for the test workstations, or at least were not identified.

But notice in this case the Red Team actually found more in terms of hardening than the Source Code Review found in terms of the documentation. Using standard Microsoft XP features, files were located and accessed that held sensitive information. In particular, the file contained the jurisdiction key, for part of the key was found in clear text. It could be opened up for the sample text director. And the key can be extracted or the portion of the key.

The Election Loader System used an Ethernet connection to install elections to the PBC units. Publicly available software was -- it was analyzing the Ethernet connections, which revealed to the Red Team that the connections used standard unencrypted protocols, suggesting that a classic "man in the middle" attack may be feasible. This is identified and described in A.13 in the summary table.

No attempt was made to exploit this attack for this test. This is another case where standard poll working -- a polling place operations and security --

excuse me. This wouldn't be polling place. This would be before it goes down to the polling place. Operational security procedures should prevent this because any of the loading within the election due to those PBCs should be conducted in a supervised, watched by multiple people, controls. It's a very short timeframe. The particular cables are tending to be very visible. They're not hidden. There's no singled access points. The timeframe's really too short to do much in terms of an exploit other than capture information.

However, as in so many other of these cases, this particular vulnerability should be corrected.

The Election Distribution CD. It was the real kicker in the whole thing. Given the ease, the Red Team was able to go ahead and crack the encryption because of a number of problems on the encryption implementation on the CD and regularly replace the CD with a false CD.

Essentially the Red Team found in the files contained in clear text the jurisdiction key; and another file, which we're not going to define for confidential reasons, that contained other information for the encryption in clear text. Using the information, the Red Team was able to -- and this is their word -- "un-obfuscate" the Data Encryption Standard (DES) key. It was actually stored using a relatively simple cipher

that's well known. In fact, it's an historical cipher. And this is the place they found the actual information sufficient to break the code within the Wikipedia on the Internet.

With this, they were able to essentially gain access to these DES keys and use the information to re-encrypt files and -- re-encrypt the Election CD with a false election definition.

The Source Code Team, without having that jurisdiction key, was also able to show that they could break down the DES key for information on the CD and create another method for attacking the DES encryption.

Essentially what's happened here is there has been some fairly good design on trying to use encryption to protect the system. But the implementation is faulty. They're using the DES and low efficient encryption standards, which most security officials identify as deprecated. It's too weak of an inscription tool. And there exists tools now available that usually can go ahead and break this in a reasonable amount of time. Not necessarily overnight but still...

On top of this, they found that the full DES was not being used. It only used a portion of the range on those particular keys. The rest of it was basically prefixed hard-coded type of information. So it's

relatively easy to go ahead and break this key. The Red Team was able to go ahead and do this, be able to access and open everything, without a lot of assistance from the Source Code Team. The Source Code Team developed a script and information to be able to go ahead and crack this in a fairly short time.

They demonstrated this particular attack, as I mentioned, by disabling the overvote detection features in the PBC by changing the Election Definition CD. They also noted, although this was outside their focus, the same method could be used to create and alter vote tallies in operations used by this. Some of those changes potentially giving access to the overall system file and operation could potentially include the use of a code to detect particular cases and turn it on and off so it would not necessarily be detected in what you can actually test.

Again, the summary table lists all of the identified vulnerabilities. I should have this memorized as many times as I looked at this, but I still need to check it. Hold a second.

There were 16 vulnerabilities, ranging from enhanced to basic, using the same functions and parameters. Again, even though this basic is considered a very low level, very vulnerable type of issue, very easy to conduct, these need to be put in perspective the actual

operating security procedures and physical security.

It's worth mentioning that no voting system is safe unless there's adequate physical security to protect.

The Red Team attack was basically a very open, uncontrolled, unrestricted access to the machine. The alarming thing about it was how quickly and how easy it was to go ahead and open this box. It wouldn't take a very large window of opportunity for someone to get in, make some changes, close it up and not be detected.

The only real delay on that is that recovering those seals requires some drying time that would make it a little bit longer than that 20 minutes to go ahead and open up the box. But this still is a factor that needs some attention.

Noel Runyan, who conducted the accessibility test, also gave me some information on the accessibility. And I want to mention one point in terms of the security testing.

The Source Code Team had one vulnerability that they identified. They took a look at the coding that was used for the audio ballot and they found that the audio files that are used for that audio ballot, there was no protection to make sure that those audio files actually matched the counters for particular candidates for the race. The result was that the person using the Audio

Ballot could be told one name and their vote would actually count for someone else.

In the same token -- No. Let's go on. The Election CD attack demonstrated the way this could be done.

The other thing was that the particular device involves a cable that goes across that connects to the PBC. That cable can be rerouted to go to another device. A blindfolder that's trying to use that would not be able to verify or check that one. This particular vulnerability may not be very serious. Again, under full operations where there's open servers, the cable is fairly short. It should be openly exposed, visible to everyone involved. I would not expect this to be a very viable method.

However, the concept in terms of where the cable was disconnected and a keyboard was attached could also involve a disconnect and connection to another PC which could take on the control of the PBC for the periods of time when it was connected.

So this is another source. The cable needs some significant procedural and physical security for it because of its potential about being able to get access or gain access to the system.

This concludes our report on the security

testing. I have to say that the Atsec people did a very, very good job considering some of time limitations on the scope of what was being done.

MODERATOR MILLER: Thank you, Mr. Freeman.

We're going to actually take a five-minute stretch break. And then there will be an opportunity for the panelists to ask any questions of Mr. Freeman.

So we shall reconvene at 11:20.

(Thereupon a recess was taken.)

MODERATOR MILLER: Back on the record.

Mr. Freeman, would you like to make some additional remarks? And we'll have some questions or opportunity to ask questions.

Mr. Freeman.

MR. FREEMAN: I have some additional material to present. I wasn't involved directly with the accessibility testing which completed last week. But I did talk with Noel Runyan, who led that particular test. He has provided a summary in the process of trying to complete the formal report. And he identified some of the issues for me to go ahead and report this morning.

That particular test was done -- they started off with about 12 people with expertise, applied juristics to the review of the system of particular problems and issues that were well known. And then completed by doing a

test -- well, I can't recall the actual the number, 30 or 40 individuals with varying levels of disabilities, including some people that would normally be considered within the normal voting population, to see how well the system behaved.

Because some issues with the system, they included within that testing not only the InkaVote Plus Audio Ballot unit, which is designed to try to satisfy the ADA requirement on the HAVA. They also included the manual marking of the ballots. Marking devices was used in the voting booklet that was used. Because in many cases there's a large portion of the population that can use the Audio Ballot, and it carries various disabilities. And there was several incidents that involved that. I'm not going to try to list all of those. It's quite an extensive list.

He identified the most shocking finding, it had to do with physical safety of the particular device. The device is normally mounted on a set of thin pipes. They were identified as about three-quarter inch. The stand designed intended for wheelchairs to go underneath. The wheelchairs, not all apparently could fit. Or he didn't give me any more specifics than that. But he did mention a wheelchair coming up and bumping those legs, they had incidents where the Audio Ballot unit actually dropped

forward and landed on the people in the wheelchair, causing potential injuries.

Also, the lid that's part of the unit lifts up out of the way, but it's not secured out of the way. It just uses sort of a center balance point where it tries to balance out. And using the bump in the system, the lid actually could slam down and cause serious damage, particularly for someone that may be blind and cannot actually see what's happening.

The other major problem was a lack of a visual display. The implementation on this particular device took advantage of an issue within the HAVA Code where they specifically named visually blind voters as an ADA category. And there's been several attempts to go ahead and identify the ADA device only used to satisfy those voters. In general, that's considered an incorrect interpretation. But my instructions and guidance from legal counsel is that issue still has to be determined in terms of state level either through legislative or rule procedures or through actual court case.

I don't know if that necessarily applies to InkaVote. That's just a general issue that's going on.

The problem with that is that the InkaVote provides no support for those that are visually impaired, though in many cases are sighted well enough that they can

use a visual screen, but they need the enhanced capabilities of the screen to show a higher contrast, variations of colors in terms of color blindness, or be able to show larger fonts, be able to show sections or subsets. There's a number of other issues that has to go with the range of visual impairment.

Some of these even get into people that are much like what's considered normal voters in terms of marginal vision such as older people with reduced vision.

It doesn't support people with hearing problems. They can't use it. And there is a broad category of people with a hearing problem that otherwise cannot use the manual marking device. Or if they do, they have some problems.

And it doesn't support the manual dexterity. There's some references to say that they could use a head stick or a mouse stick device to use the controls. But under actual testing devices, controls are not designed for that to be an effective device.

As an alternative, because of these limitations in terms of the voting population, they tested against the manual ballot, the actual marking, using the voter ballot booklet and a template device. In this particular case, the idea is that the people would go ahead, be able to read the booklet, be able to position the appropriate

marker within the hole of the template, and be able to make the mark. And they discovered even normal voters could potentially have problems with the other device, that is used for someone that can't handle a pencil or something doing this, they discovered it could be used. You think you'll need a registration with it, or when you pull the cards they found out the vote actually wasn't registered.

I'm a little bit suspicious about this one, because some of the testing we have done indicates that it doesn't take much of a mark for that to be read. But apparently from what they've witnessed within the testing, this can be a problem all of its own.

The people with manual dexterity problems and issues and with limited site also have problems being able to position those -- especially with the head sticks or positioned within the small template patterns and could potentially could be offset.

There's some other problems that occurs on the people with audio -- might potentially use the Audio Ballot. They could have some problems. Not everyone that will use the Audio Ballot is capable of following audio instructions. There's a cognitive problem that occurs in many cases. A combination of visual display and the audio ballot is necessary for them to function effectively.

They did identify some mitigations. One of the things they noticed was on the voter ballot sheet. The particular samples they had to detect instructions included a high gloss. And some people with not very acute vision had trouble reading the ballot box -- or the ballot booklet that -- with that gloss, particularly with reflected lights.

There was no provision for using larger text or fonts for those with limited site on the ballot layout. It tended to be a very small font. It potentially could be a problem. They could reposition in terms of the mitigation. The -- position, spreading farther apart so they could use a larger text in the booklet. But that requires special booklets to be produced. And the samples that were provided they used red ink for instructions. And people with dim site or with color blindness would have trouble reading those. It should be appropriate with high contrast color instead of the red.

I noticed some of the security issues in my previous report. In particular, the fact that there's no way to verify or validate a requirement under HAVA, that there should be some sort of method to be able the review a summary of how the ballot was voted and completed to confirm it was voted as the voter intended. Without the visual display or some other method, there's actually no

way to do that with the Audio Ballot device. They have no way to read the ballot, report back, other than determine whether it's overvotes or blank ballots.

I don't know if he's actually included in the report, but he also reported an area that probably hasn't being tested at all. And that is RF audio interference in the audio circuit. It turns out a simple radio nearby it. It probably does not meet a very good standard with FCC, but that's hard to tell. I was able to create enough noise that the audio signal could not be understood.

They also noticed issues in terms again with the safety at different places. The loading the ballot into the PBC.

And some other places there are sharp edges that someone that is visually impaired, including the blind voter, would not be able to notice and avoid, they could cut themselves. I'm not surprised that hasn't been identified during the safety testing.

The ballot that's actually produced by the Audio Ballot is on a paper that's carried on a roll. It comes out curled. It's not the standard quality of a Hollerith IBM card. And essentially can be read by the PBC, but it's not expected to be able to be read by the central counting device as used by L.A. Our understanding is procedurally that L.A. has proposed that they reproduce,

recreate those ballots on to a regular card as part of the process, and they don't actually count the ballots produced by the Audio Ballot. Which then there is totally another potential security issue, integrity of the vote.

That's all I had in the notes. There may have been a few other things. Mostly the -- the important thing here is the risk of some of the different disabilities, including some people that would normally fit in a normal category, not the ADA qualified that are not serviced by this particular device.

MODERATOR MILLER: Thank you, Mr. Freeman.

Are there any questions of the Panel members of Mr. Freeman?

PANEL MEMBER FINLEY: I had one question.

Early in your first presentation, you made one quick reference to an Internet link. And I wasn't sure whether -- and I may simply have misheard you. But from my reading of the report materials, my understanding is that there aren't any Internet links used as part of this system.

MR. FREEMAN: I'm not sure if -- if I actually said Internet, I misspoke. It should be Ethernet zoning linked.

Ethernet is not an Internet link necessarily. That particular connection is just a short local cable.

PANEL MEMBER FINLEY: Okay, good. Thank you.

MODERATOR MILLER: Thank you, Mr. Finley. Thank you, Mr. Freeman.

Next on the agenda I have: 3. Voting System Vendor Response to Report.

Is there anyone here from ES&S or --

Very good.

Please approach the podium and please state and spell your name.

MR. ORTIZ: My name is Chris Ortiz O-r-t-i-z. I'm the Director of Business Development for Unisyn Voting Solutions.

And we just wanted to come here today and thank you for the review you've done on our system, and assure the Panel and the Secretary of State we'll do everything we can to address these issues.

That's it. Thank you.

MODERATOR MILLER: Thank you.

Any questions from the panel members?

If not, we will move on to Item No. 4. This is the public comment period.

Let me go over briefly again some of the guidelines.

Anyone that wishes to speak that has not filled out a card, please do so. We are taking speakers in the

order of sign-in. So if you have not signed a card and wish to speak, please raise your hand and staff will give you a card to fill out.

Please print legibly so I can read with these aged -- or aging eyes. I need all the help I can get there.

I will be announcing the names of the following speaker, when I announce the speaker to present his or her remarks.

So please be ready in line. You can sit up here next to the podium so that we don't lose time with your reaching the podium.

Each speaker is limited to three minutes, except as otherwise provided for in the hearing notice. We have a very sophisticated timekeeper up here, who will indicate a 30-second notice, like that. And we hope the speaker has good peripheral vision and can catch that. And also a stop time when the time is up.

So that we can accommodate everyone who wishes to speak, I'd encourage people not to be repetitive. If someone has already made the comments you were intending to make, please just give your name, name of any organization you represent, and associate yourself with the comments previously made. This will help to ensure that people with new ideas and comments have the

opportunity to address this Panel.

While the speakers are welcome to pose questions that they hope the Secretary of State will consider over the next few days, they are not permitted to ask questions of the Panel members receiving the report or the investigators. Again, this is not a debate. This is the opportunity for your input.

I want to remind you that every comment made here orally or presented in writing is part of the public record and will be disclosed to anyone who makes a Public Records Act request.

Any additional written comments should be received by the Secretary of State's Office -- that's received, not just put in the mail -- not later than close of business this Friday, November 30th.

As mentioned at the outset of the hearing, this hearing is being videotaped and is being transcribed. At the beginning of your comments, please slowly and clearly state and spell your name. And if you are representing your organization here today, please slowly and clearly state the name of that organization.

Once more, this is a public hearing, not a debate. And I want to remind and encourage everyone to please be respectful of everyone's time, opinions, and point of view, even if you believe they're dead wrong.

With that, let's begin the public comment portion of the proceedings. I would like to begin -- and this is in order of sign-in -- Dr. Judy Alter.

Dr. Alter, would you please approach the podium.

She will be followed by Brandon Tartaglia. I hope I pronounced that right. Forgive me if I did not. You'll correct me, I'm sure.

So with that, would you please state your name and spell your name and begin your presentation, Doctor.

DR. ALTER: I'm Dr. Judy Alter. I have extended time, I understand.

MODERATOR MILLER: Yes, you do. Based upon the hearing notice, you fit within the exception to the 3-minute rule. You have 12 minutes. And you've indicated you may not even take that much time.

Go ahead. Please begin.

DR. ALTER: I'm Director of Protect California Ballots.

I'm going to report first on the ES&S precinct-based scanners and then submit to you, all in writing as well, a report on the MTS system. And I'll explain why.

This report about the ES&S InkaVote Plus precinct ballots counter and the audio device for the visually impaired and limited-English voters comes from poll

watchers, specially trained poll workers for about 248 poll sites, and 230 EIRS reports in the Los Angeles County for the November 2006 election. I reported on only one-third of these reports on July 30th.

Thirty percent of the 360 reports concerned these ES&S scanners. Ten cover the audio devices. Eight of the reports stated that the machines worked all day.

The machines did not work at all at 50 of the 101 -- in 50 of the 101 reports. They did not turn on. They jammed, becoming inoperative. Although one poll worker finally unjammed one and used it. Others described mechanical problems.

Twelve scanners worked intermittently after being fixed. One poll worker tightened a loose cable and got the scanner to turn on.

When election officials brought replacement scanners, four worked and two did not.

At the four poll sites with multiple precincts reported on, if one of scanners was missing did not work, poll workers let all the voters from other precincts scan their ballots into the working one and sorted the ballots into their respective precincts at the end of the day.

At four sites poll workers could not replace the paper roll for error messages and stopped using the scanner. At two sites observers saw that poll workers

stacked completed ballots on the floor next to the inoperative scanners instead of placing them in the ballots -- into the slot of the large ballot box.

Almost 40 percent of these scanners also had software problems. In one, the internal clock was off an hour and, thus, stopped working an hour early.

Twelve scanners rejected ballots with no overvote on them, but accepted them the second time. At one poll site a poll worker set aside 50 or 60 ballots for that reason and didn't put them in the ballot box. That's different from the other what I just described. But four poll sites poll workers chose to override the error messages when the rejection acceptance by the machine continued to happen just.

Three scanners did not print out a zero tape, and one poll worker did not want that information made public. So I rejected a ballot but did not print an error message.

Problems with the ten audio-assist devices ranged from poll workers not able to set them up to replacement devices set up by county officials that did not work after five tests. One visually impaired voter spent a half hour -- a half hour voting on one. But at the end the machine did not print out the voter's ballot. The voter voted again with assistance and left very frustrated because of the time loss.

Five voters wanted to use the ADA machine for language assistance. But when they heard it took 30 minutes, they had their children help them instead of using it.

Registrar Conny McCormack Told the poll workers who staffed the 5,024 precincts that these InkaVote Plus scanners were not tabulating votes. Remember, they have -- all right.

My team of 21 snap tally witnesses found that at the end of the day the poll inspectors printed out the tally tape for the L.A. Times and Edison exit poll reporters instead of hand-counting the selected results of the snap tallies as we witnessed them doing in June.

These snap tally witnesses verified that the software in these ballots tabulates the ballots as they are scanned in even if during the 2006 election they were officially not tabulating.

Finally, in each scanner is a modem -- interesting that this was not described in the review just now -- and we cannot tell whether it's turned on or not. Current election code bans wireless capacity and DREs, but not scanners. We strongly recommend that you not continue to use these scanners based on this information.

I'm also submitting 30 more petitions beyond the 360 I submitted in July for hand-counted paper ballots

signed by 180 more citizens, that I collected at eight more talks since July 30th, requesting that the Legislature stop using the use of secret vote counting on computerized machines controlled by private companies.

Please return to publicly counted paper ballots counted at the precincts tabulated on adding machines with no software. The mathematical process of adding numbers is not proprietary. Without ballots counted in public, we don't have democratic elections.

When L.A. County was considering the use of ES&S machinery, we circulated -- I circulated the Berkeley Consulting Report that was done about the ES&S machines. That listed almost everything that Mr. Freeman just reported to you: All the encryption problems, that you could lift the machine and slide ballots in or out, but various other things he described. He also didn't say to you what was in that report, that that machine has a modem and there's no place that you can see whether it's on or off.

Okay. We tried very hard to get them to cancel that contract, and didn't succeed obviously.

Now, I'd like to tell you about MTS. That's the Microcomputer Tally System used in L.A. County.

On June 26th, 2007, the Los Angeles Board of Supervisors approved the request by Registrar Conny

McCormack to exclude the MTS tabulating system from the top-to-bottom review of the California election systems conducted by Secretary Bowen. On November 30th, last Tuesday, she now -- the Board approved Ms. McCormick's request to use it in 2008 without its being reviewed. I actually submitted a request to Secretary Bowen to not exclude it, and submitted a simple report from the 2005 1-percent manual tally as evidence. I also sent in a letter showing that MTS has never been federally certified.

My study in 2005 looked at the exact match between the hand count and MTS-counted ballots. They matched on an average of 28 percent: 22 percent in the eight initiatives; 14 percent in local elections; and 44 in the eight little local issues.

Now I'm submitting to you a statistical report of the 1-percent manual tally of the 2006 June primary and November general election done by Brian Dolan, professional statistician. This report also shows how inaccurately MTS counts their votes. And I summarize his report. I will hand you this.

I will also hand you every report from the ES&S scanners. I brought you copies.

First, Brian did a line-by-line analysis of every entry in the report for 70 to 83 precincts. In 8,869

entries, the exact match was 81 percent, the hand counted and computer. That means 19 out of every hundred ballots doesn't get counted accurately.

There were 1,071 zeros in that 8,000 - 12 percent. So in fact only 77 percent matched. That is, 23 percent out of every 100 ballots is not counted accurately.

At the contest level, the match was 13 percent. And that's the kind of comparison I did with just simple counting. Eighty-seven percent had discrepancies. And the contest means all six candidates for Governor, each one looked at. The primary had more problems than the general election.

The manual count shows two kinds of errors made by the MTS scanners. It misses votes that the scanner does not read, if the ink dot is not dark enough or is not centered. Deborah Wright told me that. So it's not accurate that they're sensitive.

Mr. Dolan interpolated from the 1 percent across the county the rate of MTS missing a vote, that is on the ballot, is seven in every thousand votes cast goes uncounted.

But MTS adds votes that are not on the ballot, that don't exist, at a rate of three in every thousand. He found the largest discrepancy was 142 votes added in

one primary contest for this county central committee.

I only found 18 counted and added. That was the highest I found in 2005.

As a permissible error rate, Mr. Dolan used .5 percent, 1 in 200 votes. The Federal Election Commission recommends an error rate of 1 in 300,000 - .0003 percent. There's no set guideline for error rate in California.

Mr. Dolan's .5 percent error rate across the county, using that, the error rate is 1 percent. That is 1 in 100 votes counted by MTS is incorrect. We have about 3 million voters in L.A. County.

The accuracy level seen in this analysis is totally unacceptable. We have to count the ballots in L.A. County more accurately than we see here. MTS must be examined by the state experts and analyzed for its accuracy, transparency, and reliability in the same manner as the other California election systems were.

I request that you and your staff members study the analysis completed by the professional statistician Brian Dolan, showing you serious level of inaccuracy, and find ways to improve it.

Please do not replace it with any proprietary system, now shown in the top-to-bottom review to be poorly designed, inaccessible, and seriously insecure.

MODERATOR MILLER: Thank you, Dr. Alter.

Now, you have reports to submit?

DR. ALTER: Yeah, I'll give them to you.

MODERATOR MILLER: Okay. Would you please obtain those them from Dr. Alter.

Any questions from members of the Panel?

Hearing none.

Thank you, Dr. Alter.

The next speaker is Brandon Tartaglia.

Is Mr. Tartaglia still with us.

If not, we'll move on to Dean Logan, followed by Tim McNamara.

MR. McNAMARA: Can I cede my time to Dean?

MODERATOR MILLER: Yes, you can.

Okay. So six minutes.

MR. LOGAN: Good morning. My name is Dean Logan D-e-a-n L-o-g-a-n. I'm the Chief Deputy Registrar/Recorder/County Clerk for Los Angeles County.

I want to thank you for holding the hearing this morning and the opportunity to comment.

I'm going to limit my comments mainly to the focus on the Red Team report and that aspect of what we heard this morning. We were under the impression that the accessibility testing was not completed yet, and we've not had the opportunity to review that report. So I will most likely have comments on that and be submitting those

later. But since we haven't been given access to those reports, I can't comment on those today.

I'm going to cover three things. I really want to focus on context, timeframe, and service to the voters.

First, to put into contest that L.A. County uses InkaVote Plus as one of three components of our voting system. We use it for the HAVA compliance, the federal compliance to provide voter ballot protection and to provide disability access, essentially the second-chance voting component of the Federal Act as well as the disability access. It is not used for official tabulation of votes or reporting of election results. That's done centrally on our central tabulation system, and that is separate and apart from our use of the InkaVote system.

We have used the InkaVote Plus system. We Piloted it in a small number of precincts in the June 2006 primary. Then we fully implemented it in the November '06 general election and have successfully used it in nine elections in 2007.

It's also used by the City of L.A. And then it's also used by Jackson County, Missouri. Those are the three jurisdictions that we're aware of that use this system.

I want to reference in terms of context directly from the report. On the bottom of page 3 it says that the

Red Team was not trained on best practices for voting systems nor provided general guidelines for the operational, physical, or procedural security practices as practiced by the County and City of Los Angeles other than that information that was in the technical data provided by the vendor. And then it goes on to say that several of the observed vulnerabilities may be ameliorated by such practices.

I just want to point that out, because we certainly understand that that was not the scope of the Red Team testing. But in terms of the Secretary looking at the system from a certification standpoint, those operational and procedural environments in which the system is used are certainly applicable and we hope that the Secretary will take those into account.

I specifically again want to focus on the designation that Los Angeles County -- and this is noted in the report -- does not use the InkaVote Plus system to tabulate votes and report election results. It's used solely for the voter ballot protection and disability access, which is very different that other systems that the Secretary has reviewed and recertified under the top-to-bottom review.

Secondly, I want to talk a little bit about timeframe. As we stand here today, we are roughly 70 days

away from the February Presidential primary election, which from an operational standpoint means we're 60 days away from having to have precinct voting equipment ready to go and distribute to poll workers and precincts; and we're 26 days away from having to have ballots available for voters so vote in that election.

We're nearly two months following the time that the testing of this system began. And we have been in regular weekly contact with the Secretary of State's Office with regard to the testing as well as potential conditions that may be placed on the InkaVote Plus system.

So there is a time-sensitive issue here in terms of our need to move forward with preparing for the February election.

We believe, as I'm sure you did, that there was valuable information in the one report that we've been able to read. And we believe there will be more valuable information in the additional reports to come out. But so far put in context with the operational and security environment that we have in place in conducting elections and our use of the system, we don't see anything that would prevent us from moving forward with successful elections. And we would urge the Secretary to act as quickly as possible on recertification of the system.

Finally, in terms of service to voters, I think

that does need to be the focus with regard especially to InkaVote Plus how it's used in Los Angeles County. It is providing a valuable service to the voters of L.A. County. We have had some very visible and highly -- high profile examples of the InkaVote Plus system providing voters in L.A. County with a second chance to make corrections to their ballots where their vote was not recorded the first time and was read as a blank ballot or where they had overvoted, voted for more choices in one contest than they were allowed, they were given the opportunity to correct that mistake, submit another ballot. That ballot is the official record. That's the ballot that comes back and is centrally tabulated on our approved central tabulation system; not counted, not reported from the InkaVote system. The InkaVote system simply provided that protection piece.

Similarly, we've had other high profile examples of the disability access and people's ability to vote independently in some cases for the very first time using the audio ballot booth component of the InkaVote system.

So in summary, again I want to focus on the fact that with the operational environment and procedural environment that's offered to voters in L.A. County, the voter controls how their ballot is marked, how it's submitted. And then it is counted centrally at our

headquarters on election night on our central tabulation system. That ballot's available for recount. That's the ballot that's used in the 1-percent manual count that's required by state law. And there is nothing -- there is no data that is taken from the InkaVote system and uploaded for purposes of vote tabulation. That is a totally separate process.

In that context we believe that it is appropriate for there to be a different level of risk assessment with regard to how the system is used in comparison to other precinct-based tabulation systems that are approved for use in the state.

There are several things that we can respond to in writing with regard to the issue of the seals that are used. Well, we don't have any more specific information about the household chemicals that are used to remove them. I do want to point out that those are serialized seals. So even if they're removed and somebody wants to replace it with another seal, the number that was on the original seal is recorded and is logged by our office. We can go back and track that. There's a chain of custody. And we can take that machine down.

One of beauties of this particular voting system is that if there's a problem with that equipment, voting does not stop at the polling place. But voters are still

able to mark their ballot, they're still able to put it into a ballot box. And, again, it come back to be centrally counted. So it is not a single point of disruption or failure on election day.

Additionally, within the operational environment all of the areas mentioned in the report with regard to potential access to the system, there are a number of procedures ranging from surveillance cameras, on-site security, keycard access that's logged, where those people who have access to the system and who have access to the material and the programming that was referenced in this report do not have that without restrictions and without there being a record of that. And that chain of custody and that security protocol is what protects this system from the vulnerabilities, and that should be considered in the overall issue of certification.

We are -- as I said earlier, we think this is valuable information. We're going to work with our technical staff and our vendor to look at the information presented in this report and the subsequent reports that come out. But we do urge the Secretary to act quickly on recertification and to keep in context how this system is used an L.A. County and the timeframe under which we have to be prepared to conduct a very highly visible statewide Presidential primary election, and recognize the risk

that's associated with making significant and sometimes not completely thought-out changes in a process as significant as a statewide election in literally a matter of weeks.

So, again, thank you for the opportunity. And we look forward to working with you towards recertification of the system to serve the voters of L.A. County.

MODERATOR MILLER: Thank you, Mr. Logan.

Any questions of Mr. Logan?

Thank you so much.

And Tim McNamara has ceded his time to Mr. Logan.

Next speaker is Ann West. She'll be followed by Michelle Gabriel.

Ms. West, would you please approach the podium.

Thank you.

MS. WEST: Good morning.

MODERATOR MILLER: You need to talk directly into the mike.

MS. WEST: All right. I'm trying to read my notes. I'm always changing my notes.

All right. So let me just say I don't live in Los Angeles. I'm aware of their system and their problems. I'm a member of CETN and other election integrity groups, including my own county of San Mateo. But I'm just going to read out a few sentences here based

on listening to comments here.

It's apparent from Mr. Freeman's report in particular about the 16 vulnerabilities of the InkaVote system that it can be accessed and attacked readily, thereby putting elections at risk. Such startling results should be taken seriously and many more appropriate security measures be adopted.

Specifically, such startling results suggest that the 1-percent manual recount after the election must be increased significantly from 1 percent to 15 or 20 percent to validate the results. I believe that the main -- one of the main concerns in HAVA is that the disabled be allowed to use such machines to vote. It does not say that such results for both the disabled and the mainstream voters have to be accurate, only accessible -- they only have to be accessible.

For the sake of accuracy, therefore, I would suggest -- and I'm not the only one -- there must be a manual recount required that is high enough to validate the results for all voters in view of the vulnerabilities of this system.

MODERATOR MILLER: Thank you, Ms. West.

Any questions?

Hearing none.

Move on to Michelle Gabriel, who will be followed

by Jennifer Kidder.

MS. GABRIEL: My name's Michelle Gabriel M-i-c-h-e-l-l-e G-a-b-r-i-e-l. And I'm from Voting Rights Task Force in Alameda County.

I've been to many of these hearings, and what I hear over and over again is that there are obvious security holes and an ability to break into systems without source code. I keep hearing over and over again about poorly designed software, basic security flaws. I don't understand why the voting system vendors continue to do this when they continue to espouse security as one of their major design issues and why we have to keep hearing this about the systems being used in our great State of California.

But in this one, I might have misheard, but I thought I heard something new from Mr. Freeman when he was talking about the source code review, that there was some hardening possibly, but it may have been set up just for the test. And I don't know if I heard that correctly.

But if so, I would really request that the state make sure that this software is the same software that is in escrow and that it really matches.

I also heard that hash codes would be changed to make it look like it was the same when it really wasn't. So I would really request that this be checked very, very

carefully and verified what I heard. But since I can't ask anybody at this, I can't really check.

I would ask about functionality and reliability of this system. Nobody else that I know of in this state has a system where a ballot has to go through just to check whether it's blank or not or overvoted, and then has to go get centrally tabulated someplace else. What I understand about the functionality that Mr. Logan said was that this will check that it would be read correctly. But I don't understand how, when you read something on the InkaVote system, that that's assured to be read properly at the central tabulation. I'm unclear on whether it's the same equipment and you can actually read it there.

And I would also ask about -- especially I keep hearing registrars of voters bring up about that they have different security mitigations to prevent these and that all of these Red Team attacks and source codes don't look at that. I would like to ask the Secretary of State who evaluates the operational, physical, and procedural security practices, who is qualified to do that, how do they test it, how do they know that these are being implemented properly? And my understanding is that you have to do "plan, do, check." That's what I had to do when I was in corporate America. And I hope that that's done here with at least security mitigations.

All these problems don't even have to do with the tabulation, which is the most important part of the system. And I hope that that's going to be checked and not be dropped because the software was submitted later. Especially in a county that's 25 percent of the votes, I think it's really crucial to make sure that the tabulation gets checked.

Thank you.

MODERATOR MILLER: Thank you very much.

Any questions?

If not, thank you very much.

Our next speaker after Ms. Kidder will be Jim -- I can't read this well -- It's Soper, Sopes?

MS. KIDDER: Soper.

MODERATOR MILLER: Soper. Very Good.

Ms. Kidder.

MS. KIDDER: I wanted to know if I could take one minute of my time and cede two of it to my on honorable friend Jim Soper. Is that possible.

MODERATOR MILLER: Yes, that's fine

MS. KIDDER: Awesome. Okay.

My name's Jennifer Kidder. I am with the Voting Rights Task Force and other things.

And the main reason that I felt compelled to come here today is I'm very much in support of the Secretary of

State's lawsuit against this company, ES&S, and I'm a little bewildered as to why ES&S is even in the running for certification of anything and is not being driven out of the state. I don't know why they are allowed to be up for certification on any model of any voting machine of anything when they have broken the law clearly.

And so that's -- and are they the ones who did not even submit their stuff for Red Team testing the first time around? Because this is unacceptable.

And the other thing that I noticed about this particular system, being a disabled person myself, this thing about -- as soon as I ever heard about these auditory supposedly help people to vote systems, this is not voting. This is being granted the experience of pretending that you're voting. If what you say and hear has no, necessarily, relationship to what vote is being recorded and cast on your behalf, I find this outrageous. You could be listening to Bud Travis albums in there for all it matters, it seems to me.

And, you know, I want to Berkeley because it had a 10 percent of the population disabled, and I thought that was great. And this is a huge population. It can swing an election, not to mention the individual rights of those people and myself having our votes stolen.

So thank you.

MODERATOR MILLER: Any questions?

If not, Mr. Soper. And Mr. Soper will be followed by Judy Bertelsen.

MR. SOPER: Thank you. Good morning. My name's Jim Soper S-o-p-e-r. I'm a senior software consultant and the author of a website called countedascast.

First of all, for the audience that may not have been able to evaluate these reports, I find them rather professional and want to compliment the team. They appear to be very well done. Thank you, Mr. Freeman and your team.

And also, as a summary for people who couldn't get through the technical stuff, these machines are highly vulnerable to insider attack. It's a summary. And I mean they can open up the box. They can do all kinds of things people have done with these machines, just like the others, can get at them.

Now, they are not used for counting, and that's good. Except that I think I would like to suggest to Los Angeles County and Mr. Logan that they do use them for backup counting and double-check counting. You get the -- I mean they were talking about doing zero tapes at the beginning of the day. Well, somebody's counting something if they're using zero tapes at the beginning of the day.

If you get those tapes out from the precincts,

and what happens if the ballots get lost on the way back to the headquarters, whatever. You use them to double check the numbers. So I think it would be good if they were not the official count but a double-check count. But then they should -- all systems should be reviewed with that in mind.

What disturbs me probably the most is that this was done as one system in isolation from the rest of it. And I'll give you two examples. One, is there's XML code coming into the InkaVote system. One, we don't know what kind of media it's coming in on. Is it encrypted, is it not, et cetera.

XML is normally used data and could theoretically in principle not corrupt -- does not have a program in it that, in principle -- if it's just data, it could not corrupt the scanner system.

However, XML also allows for scripting, which is programming, which is not allowed. And if you have one people looking at one system that's producing an XML file, and they said, "Well, maybe there's some scripting in there," but they're not paying attention to what's going on as to what -- how it's going to be received because that's in another box, then you have a vulnerability and you've got a problem. You need to look at the whole thing.

The other part is what Ms. Alter brought out, is you have these ballots that are marked by InkaVote, and in the case of the MTS we have a very high rate of incorrect readings by the MTS system, and that's worrying and that's because you're not checking the whole thing. I think what the State of California needs to do is once you work out what L.A. is going to use, you run a volume test on the whole thing end to end. When I was coming here a couple years ago they were talking about having to do everything end to end. And I think that needs to be done here, is to do everything end to end with volume testing, because we have indications that the volume -- it may not be very reliable.

The certification, this should be just for the use as L.A.'s described and no more than that, so nobody else can start to use it for other things.

The things about the use of a modem worry. There being a modem in the machines is very possible. A lot of standard computers have modems standard on them. They should be disabled by removing the jumper.

The not using logs, the SQL, need to be checked more carefully.

And I would like to know if the Java is compiled or interpreted. Not saying that they shouldn't use Java, but we need to know what we're dealing with.

Thank you very much.

MODERATOR MILLER: Thank you, Mr. Soper.

Any questions?

In not, thank you.

Judy Bertelsen, followed by Kathay Feng.

MS. BERTELSEN: My name is Judy Bertelsen J-u-d-y B-e-r-t-e-l-s-e-n. And I'm a voter in Alameda County and I'm a participant in the Voting Rights Task Force.

Mr. Freeman has outlined today extensive security problems that have been known for some time, as Judy Alter and others have noted. And these problems should long ago have been mitigated or corrected.

There remains a question of how the votes actually are tabulated. We are told that InkaVote does not tabulate them. And so this specific Red Team inquiry didn't look into the tabulation. But we do need -- as Jim said, we need to know how the whole system works.

We are told that InkaVote has counting and tabulating capability. But Mr. Logan said that it is not used for official tabulating. There seems to be some indication that it is used for unofficial tabulating. We've been told by various observers of L.A. elections that they see evidence of tabulation results. And we hear that they have been given to the press or to possibly exit poll participants.

So my concern is that -- well, just what is this tabulation used for? And also, why isn't it -- since it is a capability and since apparently it is being used but not for official tabulation, why should it not be used as a part of an audit procedure. This would be unique to this particular system. But it seems to be a very obvious, easy thing to do, to systematically save and collect the audit -- I mean the tabulation results from each of the precincts, and then compare those results with what is found by the central tabulator.

The third point I want to make is that by Dean Logan's testimony -- as I understand it, he said we are 70 days away from the election, which means 60 days away from, I think he was saying, distribution of the materials to the polling places. And that implies that there are 10 days of a long sleepover that may occur, which would give ample time to make use of the many security problems that were outlined by Mr. Freeman. It was suggested that some of these may not be so worrisome if there are mitigations because time would be needed. But it sounds like there's more than enough time to make use of these.

Thank you.

MODERATOR MILLER: Thank you very much.

Any questions?

If not, our next and final speaker is Kathay

Feng.

MS. FENG: Thank you, Tony. Kathay Feng with California Common Cause. And I'm wondering if I can take some of Brandon Tartaglia's time. He wasn't able to stay through the hearings. But I have a letter that's been signed by a number of different organizations that includes Brandon's organization, Protection & Advocacy.

MODERATOR MILLER: Why don't you go ahead.

MS. FENG: And we e-mailed this letter to the Voting System Task Force. It is signed by California Council for the Blind; Mexican American Legal Defense and Education Fund (MALDEF); my own organization, California Common Cause; New America Foundation; Asian Pacific American Legal Center; The Disability Rights Legal Center; and Protection and Advocacy, Inc.

I come here today as an actual voter from Los Angeles, not Alameda, not Austin, not anywhere else. I vote in Los Angeles. I have voted on the InkaVote system for many, many election cycles as well as monitored elections during a lot of election cycles.

Prior to InkaVote, California -- or Los Angeles used the system that was very similar, that punched through the hole, but in essence used the same device that you slip a ballot through, the same style of ballot, and that California Common Cause actually sued to remove

because of serious concerns about voter errors.

And so today I bring a very nuance message. I am not a fan of InkaVote. It has serious disability concerns. It has serious problems in terms of voters who need multi-lingual assistance. I don't know if you all have handled the marking device. But when you slip the ballot in, often times voters don't slip it all the way in so the little bubbles don't match up or align perfectly with the pages. And so they can make mistakes. Or that's why when they mark, the mark doesn't go all the way through. It ends up being a half moon, and there are problems with that. It's not an uncommon problem and it's why a lot of times voters have to mark it multiple times.

We have concerns about voters with language abilities being able to use these machines -- or these marking devices, because it is in essence an English-only system. The bubble -- the ballot itself is just numbers and bubbles. So there's no way of looking at that and being able to be sure that the bubble that you marked really matches up with the candidate choice or the proposition choice that you wanted. In many ways, its like a scantron that you might have used if you took the SATs way back when, where if you're one bubble off, everything is misaligned.

And voters with language abilities have a problem

because the marking device that they slip it into is English only. And, again, in order to vote using a multi-lingual -- some type of multi-lingual assistance, they'd have to hold a translated ballot -- sample ballot next to the English ballot and go back and forth and back and forth. And you can see where your mistakes can start to happen in terms of aligning the bubble correctly. If you don't do it right, it will all be off.

There is the audio capacity. And certainly that helps a great deal. And for voters who have disabilities or need the language assistance, at least they have some backup systems to be able to go and listen to the entire ballot. But it's a cumbersome one. I mean you have to listen to the whole thing being read. And if you really wanted to just skip to question number whatever, or if you weren't sure about a particular race but you wanted to move ahead, you still have to fast forward through the whole thing, much like a VHS tape. It isn't as user friendly as some of the other systems.

So all of that said, the organizations that are signing on to this letter today still want to urge that this task force think very seriously about the certification of InkaVote, particularly because we're two and a half months away from an election. And L.A. County is too big of a county, with too many voters, too many

poll workers -- 5,000 poll sites, 25,000 poll workers, and 25,000 machines per -- or marking devices per poll site to distribute, to try to do a switch over.

So we're particularly concerned that not only should InkaVote be recertified, but also recertified with conditions that don't make it impossible for the disability access features to still be used.

That said, we do think that as a long-term matter, the Voting Systems Task Force should look at creating with Los Angeles County and with the many organizations that are signatories to this letter clear guidelines for development of a long-term process for replacing the InkaVote system.

Conny McCormack has often times said that InkaVote was only supposed to be a transitional system. She wanted to get off of punch cards. It's a big county to change over fully. It would have meant a $100 million investment, which at the time she probably had a lot of foresight in not switching over entirely because a lot of the voting systems were under a lot of change and flux and certification questions, and so she chose not to.

Even so, it is important for us to think about a long-term process for getting to a new system, because InkaVote is not a system that is accessible. It certainly isn't one that is fully functional.

Lastly, this isn't directly the purview of today's hearings, but we do want to just say that we are concerned about the 100 percent manual tally requirement for the -- during the canvassing period for the Diebold AccuVote touch screens, which are used for early voting. There are fully 60,000 voters who voted early voting in Los Angeles on these machines who use it because they need disability access, because they need language assistance, or because, frankly, it's just convenient. And having a hundred percent manual tally would in essence require L.A. to give that up. So we would ask you to reconsider that requirement.

Thank you.

MODERATOR MILLER: Thank you, Ms. Feng.

For the record, would you please spell your name for the reporter.

MS. FENG: First name is K-a-t-h-a-y, last name is Feng F-e-n-g.

MODERATOR MILLER: Thank you.

Any questions?

Thank you.

This does conclude the hearing. I want to thank you for participating.

Written comments, if any, should be submitted so that they are received by the Secretary of State by

Friday, November 30th. That's this week.

Thank you so much for coming.

Have a good day.

(Thereupon the Secretary of State's public hearing adjourned at 12:21 p.m.)

CERTIFICATE OF REPORTER

I, JAMES F. PETERS, a Certified Shorthand Reporter of the State of California, and Registered Professional Reporter, do hereby certify:

That I am a disinterested person herein; that the foregoing Secretary of State's public hearing was reported in shorthand by me, James F. Peters, a Certified Shorthand Reporter of the State of California, and thereafter transcribed into typewriting.

I further certify that I am not of counsel or attorney for any of the parties to said hearing nor in any way interested in the outcome of said hearing.

IN WITNESS WHEREOF, I have hereunto set my hand this 4th day of December, 2007.

JAMES F. PETERS, CSR, RPR
Certified Shorthand Reporter
License No. 10063