U.S. ELECTION ASSISTANCE COMMISSION
PUBLIC HEARING ON
THE USE, SECURITY, AND RELIABILITY OF ELECTRONIC VOTING SYSTEMS
MAY 5, 2004

STATEMENT OF WILLIAM F. WELSH, II
FORMER CHAIRMAN, CURRENT MEMBER OF THE BOARD
ELECTION SYSTEMS & SOFTWARE

Chairman Soaries, Vice Chairman Hillman, members of the Commission. Good morning. My name is William F. Welsh, II. I am here today in my current capacity as a member of the board of Election Systems & Software. Previously, I've served as Chairman of the Board and President of ES&S.

On behalf of ES&S, thank you for the invitation to appear at this first public hearing of the Commission. The issues you are addressing are of critical importance to the future of elections, and we very much appreciate the opportunity to share our views. In fact, we hope this is the first of many discussions we will be having about the usability, reliability, and security of electronic voting. From our perspective, it is forums like this that will foster a climate of trust and openness and encourage constructive dialogue, versus the current debate in the media. We value the exceptional contribution you are making to the election process and look forward to working with you and your staff.

I have been involved in the election industry for more than 10 years – and in my various roles, have driven the evolution of today's voting solutions. I have to say, it's been an incredible experience. There is nothing more awesome or fulfilling than supporting our democratic process. It is the essence of who and what we are as a nation … and, it touches every one of us, every day. All of us at ES&S appreciate the significant responsibility we have to voters, around the world.

ABOUT ES&S

Turning to our discussion today, I would like to take just a few moments to provide some background about our company, our products, and – importantly – our approach to ensuring the security and integrity of the voting process.

As you may know, we have more than three decades of experience in innovating voting solutions. We're very proud of and take seriously our role in the democratic process. Maintaining voter confidence – and enhancing the voting experience – is at the core of our mission as a company. When people ask me what our greatest strength is, I always get the impression they're expecting a long-winded recital of our technical know-how. While that is impressive, I think I surprise them when I simply say we have the most dependable, most knowledgeable election experts in the industry.

Based in Omaha, Nebraska, and with roots going back to 1969, ES&S has sustained a well-honed focus on carrying out our ***sole purpose*** as a company – offering the best and most reliable voting solutions to voters and elections administrators around the world. Today, we partner with a customer base of more than 1,700 jurisdictions in 45 states, serving more than 50 percent of the precincts and registered voters nationwide. Since our inception, we have supported more than 40,000 elections, tabulated millions of ballots, and offered ever-improving elections solutions to the voting public. Here in the U.S. alone, we have installed or have contracts to install nearly 50,000 direct-record-electronic voting machines.

ES&S offers the election industry's only end-to-end voting solutions – from our voter registration, candidate filing, and election management software; to our optical scan and iVotronic touch screen voting equipment; to our centralized tabulation systems and a proprietary results reporting process. As a business, elections are all we do. And, through a passionate commitment to innovation, ES&S has taken one of the world's most important traditions – casting a vote – and transformed it into a 21st century high-tech process.

USABILITY

The results – and benefits – of a move toward electronic voting have been outstanding. From the voters' perspective, electronic voting has made the election process easier, more accessible, and even a bit more fun. It has also made it much more reliable because we have eliminated the potential for over-votes and, through a selection verification screen, provided voters an opportunity to confirm their choices before a vote is cast. When it comes to capturing voter intent, electronic voting has moved us light years ahead.

Electronic voting has also provided new opportunities to voters who previously have been disenfranchised. The audio function on our iVotronic DRE machines provides to visually impaired voters the first-ever opportunity to vote unassisted. The lightweight and portable feature of our iVotronic makes it possible for those in wheelchairs to cast a ballot curbside or by using equipment placed in their lap. And, because our iVotronic DRE machines support ballots in many languages, electronic voting is encouraging participation by voters for whom language has been a barrier.

Where optical scan voting is utilized, ES&S has announced a very exciting new product – the ES&S AutoMark – which makes it possible, again for the first time, for visually impaired voters to cast optically scanned ballots privately and independently. All of these improvements accomplish one very important and over-riding goal – enhancing the voting experience for *all*.

And, for election administrators, the benefits have been just as profound. Elections are run more smoothly. Results are tabulated more quickly. Data is managed more efficiently. Take, for example, the results of a recent assessment of a 12-month electronic voting pilot project in Bexar County, Texas. There, we installed a complete electronic voting system and conducted four successful elections. According to the county's official report:

- 146,472 votes were cast without losing a single vote.
- Early results were reported by 7:15 p.m.
- 90 percent of the count, or better, was reported by 10:00 p.m.
- There was no shortage of ballots.
- And, the county experienced a high degree of public acceptance.

The fact that ES&S is on the forefront of innovating technical solutions is something of which we are very proud. Even so, while current election technology is more high-tech than ever before, our core values at ES&S have always remained the same. The principles of security, accuracy, and reliability are – and always have been – at the forefront of what we do, every day.

SECURITY

We know, however, because of the newness of today's technology and natural skepticism when it comes to change, some are questioning the security of today's electronic voting options. On the issue of security, I am reminded of a comment in Dr. Michael Ian Shamos' well-known paper on evaluating the threat of electronic voting. In that paper, Dr. Shamos wrote:

> "[T]he effort expended in meeting threats to the election process should be rationally related both to the probability of the threat and the seriousness of its effects. No one would buy a safe that could easily be opened, but everyone who has ever bought a safe has bought one that can be cracked. The same is true for voting systems. The issue is not whether they are secure, but whether they present barriers sufficiently formidable to give us confidence in the integrity of our election."

I couldn't agree more with Dr. Shamos. And I believe electronic voting has passed Dr. Shamos' test – it does provided confidence in the integrity of the election process. Based on thousands of election results generated through electronic voting machines, we can say with certainty that the equipment used today by ES&S is absolutely secure. But, we're not simply saying "trust us." We've taken very real steps to demonstrate and ensure the security of our systems.

At ES&S, we believe very strongly that security measures must be built into the entire election cycle – *before*, *during,* and *after* an election. This includes important processes and procedures, training and education, and other steps to recognize the extremely important human aspect of carrying out an election. This is a business which relies on human beings to do their jobs, effectively and efficiently, and at ES&S we work very hard to ensure that this element of the voting process is carried out successfully. On a technical level, we have integrated into our systems comprehensive and complementary checks and balances to ensure the security of the process – including very sophisticated and detailed specifications in the development and design of our hardware and software.

And, our own internal checks and balances are complemented by the very exhaustive and stringent requirements established by this body and other government agencies at the state and federal levels. The truth is that before any of our equipment may be used in any election, it must pass a thorough and rigorous review by independent testing authorities, charged with demonstrating that our equipment meets or exceeds government standards. The ITA testing and certification processes verify that our systems meet federal and state requirements on a number of fronts – including source code, hardware, software, environmental, functional, logic, and reliability.

Then, as you know, often times ITA testing and certification is backed by an additional layer of checks and balances – with a thorough assessment conducted at the state level, as well. This certification and testing process is complex, complete, and absolutely critical to ensuring the integrity of today's voting solutions.

Unique Security Features Set Apart ES&S Equipment

Nonetheless, even with these strong protections provided by the common standards that govern equipment used industry-wide, at ES&S we have taken this commitment to security one step further. There are a number of unique security safeguards that set apart ES&S' touch screen voting technology from the rest. This includes:

Personal Electronic Ballot

The iVotronic is activated by a unique personal electronic ballot (PEB) which is more secure than other activation options. The PEB is the portable data bank which holds the ballot styles for the election. In most cases, the PEB is inserted by the pollworker, the appropriate ballot for the voter is automatically downloaded into the iVotronic. (The iVotronic also has the flexibility to be voter-activated.) When the initial screen comes up, the PEB is removed and the voter will follow the on-screen instructions to begin voting. Quite different from technology like a PCMCIA card that is used in other types of DRE systems, the PEB is unique, patented technology that is not commercially available. The PEB is not open to either wireless or wire-based systems and does not allow Internet connections, direct phone line connections, or direct network connections – all features that help protect the iVotronic from any kind of outside manipulation.

Both the personal electronic ballot (PEB) and the port are designed by ES&S and incorporate proprietary infrared communication. The physical size and shape of the port is different from any commercially available communications port. This alone prevents just any device from being placed in the port. Also, the proprietary infrared port and communication protocol can only be activated by an ES&S PEB.

Flash Card Slot Security

While data on the iVotronic DRE terminals is stored on three independent but redundant memory chips, the terminal also features a removable compact flash card to supply additional memory. The card inserts in the rear of the unit and a security seal is placed on the compartment door to prevent and/or detect any unit tampering. Seals can also be placed on the iVotronic voting booth and communications pack to prevent opening of the unit and gaining access to voter terminals and PEBs without detection.

Proprietary Software

The ES&S iVotronic uses a proprietary operating system that is unique and secure, not one that you can "buy off the shelf." The advantages of this approach are three-fold: first, this type of proprietary operating system is much more efficient and compact because it is built specifically to operate the iVotronic DRE. Second, this type of proprietary platform is much more tamper-proof because, as independent assessments have shown, it is less susceptible to hacking or other security breaches. And, third, this type of operating system is much more secure because it does not support "plug and play" devices or other peripheral equipment which would be compatible with commercially available systems.

Ensuring Security … Before, During, and After an Election

Before an Election

- *Clear and Test:* A supervisor PEB cannot open voter terminals for voting until they have passed the "cleared and tested" function on the password-protected service menu. This test ensures that the public count resets to zero before any new election activity.

- *Qualification Code:* The iVotronic system also employs an election specific election qualification code (EQC) that provides system-wide security. During preventative maintenance, a single supervisor terminal electronically generates an election-specific EQC. This EQC is then transferred via the supervisor terminal to all Election Day and early-voting PEBs. Next, these PEBs download the election-specific EQC into terminal memories when individual voter and supervisor terminals are cleared and tested. Thus, in order to activate for voting, the PEB and terminal must contain the same EQC. This EQC ensures that all equipment used in an election has been through the proper preventative maintenance. Most importantly, this EQC system prevents "pirate" PEBs or terminals from being entered into the system. If such an attempt is made, the system documents the attempt in the event log for audit purposes.

- *Focused Security:* Voter terminals will not allow voting until properly opened by the supervisor PEB, a specified number of which are programmed with ballots. These supervisor PEBs are distributed to precinct officials separately from the voter terminals. This process places election security in the hands of the trained precinct officials, instead of solely on those at the equipment storage facility.

- *Detect Pre-existing Vote Totals:* If a supervisor PEB already contains votes, it cannot open a voter terminal in the normal manner. A supervisor PEB normally stores votes at the end of the election, not when the voter terminals are being opened for voting. Therefore, if a supervisor PEB contains votes, that supervisor PEB already has closed at least one voter terminal and holds a copy of that terminal's vote totals. If this supervisor PEB continues to be used in the current election, these existing vote totals would be reported on the precinct results. To avoid error, the voter terminal always checks the supervisor PEB for pre-existing vote totals. If a supervisor PEB already contains votes, the voter terminal issues a message on its screen alerting the precinct official. The voter terminal then requires entry of a precinct-specific override password before the terminal will open for voting. This requirement assures that the situation will be called to the precinct official's attention and would allow a precinct official to not use that PEB, if necessary.

- *The Public Count:* The voter terminals display their public count on the screen when powered up by any PEB. Precinct officials can and should check that the public count is zero when opening the voter terminals for voting. In addition, the public count can be used throughout Election Day to cross-check against the number of voters recorded in the poll book. Additionally, the protective count present in each terminal can be verified against the public count.

- *Voter Terminals Must be Zero to Open:* If the public count is zero, the precinct official should receive the following message when inserting the supervisor PEB in the voter terminal to open it for voting: "Open terminal now for above named polling location?" If any votes already exist on the voter terminal, the public count displayed on the screen will not be zero and the precinct official would instead get one of the following messages: "Do you want to close this terminal?" or "Do you want to recollect the votes?"

If the precinct official receives the "want to recollect?" message, this voter terminal has not been "cleared and tested" since the last election. If the precinct official receives the "want to close?" message, the voter terminal is already open for voting and may or may not have votes on it, depending on the public count. This open terminal may be the result of attempted vote fraud; however, it is more likely this message is the result of elections officials testing the voter terminals in advance of the election. They may simply have neglected to close this particular voter terminal after testing.

In both cases, the precinct official will need to have trained service personnel clear and test the terminal before using it in the current election. Service personnel are required because of the password-protection feature of the voter terminal service menu as well as the "clear and test option itself.

- *Opening Date and Time Recorded:* The iVotronic system limits access to the "set date and time" feature via password-protection. Time and date stamping occurs throughout the iVotronic election process including each terminal opening date and time. Each voter terminal always records the exact date and time that it was opened for voting. Additionally, the precinct report includes the opening date and time for each voter terminal as well as the date and time the report tape was printed. Finally, the current date and time setting displays every time the voter terminal is powered-up by a PEB.

During an Election

- *Override Password Needed to Close Polls Early:* As an added precaution against potential pre-election vote fraud, voter terminals cannot be closed and have their votes collected before the official election closing date and time without the precinct-specific override password that accompanies the ballot. This override password is selected and programmed into the PEBs by election officials prior to Election Day. To close the polls in pre-election testing, election officials need access to the override password for each precinct to be tested.

- *Limited Master PEB Exposure:* Typically, each precinct has only one master supervisor PEB on site. Precinct officials always maintain possession of the master supervisor PEB, which is critical to running the election. The master supervisor PEB opens the voter terminals for voting at the beginning of the election, cancels or casts any unfinished votes if necessary, closes the polls, collects the votes, and issues the precinct report. At all other times, the master supervisor PEB remains idle in a secure location.

- *Check the Ballot:* Voter terminals check the incoming ballot for the same unique ballot qualification code that was programmed into the supervisor PEB, which opened the terminals for voting. If the ballot is not coded for the specified precinct and election, the terminal will not accept it for voting. Instead, the terminal will issue an audible alarm and display a message explaining that the PEB has not been qualified properly and cannot be used in this election until it has been reprogrammed.

  The iVotronic system also requires verification for voter-activated PEBs. Before the supervisor terminal loads a ballot into a voter PEB, it checks the voter PEB for the unique ballot identification code from the ballot last loaded into the voter PEB. If no previous ballot identification code exists on the PEB, the supervisor terminal loads the ballot normally. Similarly, if the ballot identification data on the voter PEB matches the ballot identification code that is about to be loaded onto the voter PEB, the supervisor terminal loads the ballot

normally. However, if the ballot identification code in the voter PEB does not match the unique ballot identification code for this precinct and election, the supervisor terminal issues an audible alarm and displays the message that this voter PEB has not been properly qualified since the last election and cannot be used in this election until it has been qualified.

- *Password Protection:* Password protection restricts access to the service menu and the election central application menu. These menu passwords differ from the precinct-specific override passwords that precinct officials need in the event of a deviation in the election process. The ballots for each election contain different precinct-specific override passwords (i.e., the passwords change for each election). Typically, elections officials do not divulge the menu passwords to precinct officials. If precincts require the service menu or elections central applications menu passwords, extenuating circumstances exist and trained support personnel should be present at that precinct to oversee the situation.

After an Election

- *Accountability:* The single supervisor PEB used to open all voter terminals at the beginning of the election also produces a "zero tape," a printed log that shows which serial number terminals were opened, exactly what date and time they were opened, and the number of votes on each voter terminal when it was opened – which, by definition, should be zero.

- That same supervisor PEB closes all voter terminals and collects all votes. Because the supervisor PEB recorded the serial numbers of all opened voter terminals, it requires that all opened voter terminals also be closed. This feature assists precinct officials in ensuring no terminals were inadvertently missed. If a reason for not closing a terminal develops, the precinct official can enter an override password and proceed normally. However, the precinct report still includes the serial numbers of any unclosed voter terminals and lists them as "not closed."

- *Closing Date and Time Recorded:* Voter terminals include their closing date and time on the master supervisor PEB when closed. The supervisor PEB then reports the closing date and time for each voter terminal directly beneath its corresponding opening date and time on the precinct report. This inclusion allows election officials to audit when each voter terminal at a precinct was opened and closed on Election Day. This data can also be compared to the zero tape, which was produced during the opening process.

- *Must Close Voter Terminal to Read Votes:* The supervisor PEB first must close a voter terminal before it can collect the terminal's vote totals. Once closed, the voter terminal cannot be voted on again until it is cleared and tested and opened for voting. When a supervisor PEB closes a voter terminal, the voter terminal reads the supervisor PEB first to see if this supervisor PEB has already closed and collected vote totals for this serial number voter terminal. If it has, the voter terminal will not copy its vote totals to the supervisor PEB.

- *Physical Security:* Seals are placed on the iVotronic voting booths to prevent opening of the unit and gaining access to the voter terminal without detection. Physical security (i.e., locking and security) is also important. Many of our clients, for example, provide extra security for programmed PEBs as these, after all, contain election ballots. These should be provided the same level of protection as any printed ballots. Similarly, once terminals are "cleared and tested" and implanted with the new EQC, any attempt to tamper with individual terminals will be detected.

Human factors must be taken into consideration, as well. As with automobiles, for example, safety does not rely solely on the way the vehicle is built. Safety also depends on the way the car is driven, the way other drivers operate their vehicles, and on the laws that govern vehicle design and operation. While the way the car is built is very important, it is not the only factor.

So, at ES&S, we work very closely with election administrators to train and educate those who carry-out elections about the voting systems and the processes and procedures we have established to maintain the intregrity of the voting process. It is the combination of the security features built into our systems and the on-site election support services, training, and documentation that ES&S provides to county and state election administrators that results in a secure, reliable, accurate voting solution.

RELIABILITY

As an extra precaution, ES&S has incorporated into our iVotronic touchscreen devices a unique internal audit system that provides an extremely reliable verification mechanism. This audit system includes two separate audit trails within our redundant memory functions. One audit trail captures all of the "voting events" – that is, the date and time a vote is cast. The other stores a ballot image of every ballot cast.

This separation of audit trails ensures anonymity of the voting process, while providing an extremely reliable method of replicating the entire election process. In fact, through this internal audit system we can produce ballot images to re-verify every ballot cast in an election. Importantly, after the polls are closed, results from a PEB are cross-checked against these audit trails to confirm – once again – that all of the votes that have been cast are counted. Excuse a brief brag … but, I take great pride in the fact that the ES&S iVotronic is the only DRE on the market today with this cross-verification process.

For all of these reasons – the security and audit features of our electronic voting systems, our very strong track record of carrying out successful elections, and the procedures we strongly encourage to reduce human error – I will say again with confidence that the voting equipment used today by ES&S is accurate, secure, and reliable. Nonetheless, we understand that some are considering the option of a voter verifiable receipt and, though we believe this option is not necessary, at ES&S we are prepared to respond. After all, ES&S is in the business of providing systems that our customers need.

At this time, ES&S has developed several prototypes of potential voter verifiable receipt technology. All of these prototypes provide the opportunity for a voter to see, on paper, the voters selections before a ballot is cast. What final form our voter verifiable receipt technology will take depends on the specifications and requirements dictated by the federal and state governmental bodies currently considering this option. But, should the decision be made to move forward with a voter verifiable receipt requirement, ES&S stands ready to deliver.

Conclusion

So, in conclusion, let me just thank you once again for this opportunity to present our views to the commission. You have an important role in determining the future of elections, and we welcome the opportunity to work with you to ensure that our citizens are provided the best possible voting solutions. All of us at ES&S are firmly committed to maintaining integrity of the voting process, and enhancing the voting experience for all.