Testimony before the Subcommittee of Information Policy, Census, and National Archives, Committee on Oversight and Government Reform
April 18, 2007

John Groh, Chairman, Election Technology Council

My name is John Groh and I am a Senior Vice President with Election Systems & Software. I am here to provide testimony on behalf of the Election Technology Council (ETC). The Election Technology Council consists of companies which offer voting system technology hardware products, software and services to support the electoral process. These companies have organized as an association to work together to address common issues facing our industry. Membership in the ETC is open to any company in the election systems marketplace.

The historic General Election of 2000 led to the largest election reform legislation in the nation's history, "The Help America Vote Act" of 2002 (HAVA). At the very core of this sweeping legislation was one goal, "***to ensure that every vote counts*".** This testimony is intended to provide insights and discussion points from the ETC members to concerns about the security and reliability of electronic voting systems, vulnerabilities in the development of system software code, and industry challenges to developing more reliable accreditation and certification programs for systems.

The members of the ETC have provided election services and products to thousands of voting jurisdictions over the past several years. In addition to providing equipment and services, ETC member companies invest millions of dollars in research and development every year to help improve the quality, accuracy and credibility of elections. Collectively we serve more than 95 percent of all election jurisdictions in the U.S. The members believe that elections should be accurate, secure, accessible and transparent and are dedicated to continuous improvement and the evolution of our products and services to continue in the achievement of our goals. The 2006 general election demonstrated the effective utilization of electronic voting stations (many with voter-verifiable paper audit trail printers) and optical scanners. The members of the ETC are committed to continuing to serve as stakeholders and partners with election officials to ensure that the mandates of HAVA are complied with in full.

Security

Security is an essential element of any election. As a community, election systems vendors routinely work to incorporate into the voting systems we produce security features to maintain the integrity of an election. Further, collectively, we are firmly committed to contributing to the national dialogue about how we can continually enhance our systems. At the same time, it is critically important to recognize that "security" involves much more than the technical aspects of voting equipment. To truly maintain security – regardless of the type of voting technology – one must recognize that security is an end-to-end process and account for the "totality of circumstances" that can impact the integrity of elections. The fact is that processes, procedures, testing, training … *and* technology all play important roles in maintaining the security of an election.

In recent testimony before the U.S. House Committee on Appropriations, Donetta Davidson, Chair of the Election Assistance Commission (EAC) stated,

> "fundamental election administration processes to protect the entire voting process will always be important, even as voting technology evolves. Focusing solely on the reliability of voting systems is not enough, and Federal certification for the system cannot take the place of solid, thorough management procedures at the State and local levels to ensure the system is managed, tested, and operated properly. Achieving accurate and reliable election results will always be the combination of thorough testing of the equipment at multiple levels, training and resources for election officials and poll workers, and through election management guidelines for every aspect of election administration."

We could not agree more and strongly encourage all members of Congress to keep in mind this totality of circumstances concerning security. Whether it is setting up best election practices at the state level to chain of custody security procedures at the local level.

To learn and understand more about the end-to-end security processes that need to happen for successful elections reference the attached testimony from Ms. Donnetta Davidson, Chair of the U.S. Election Assistance Commission before the U.S. House Committee on Appropriations, Subcommittee on Financial Services and General Government, March 7, 2007. (Attachment A) Also, attached is a white paper from the Election Technology Council concerning election security, Election Security: Totality of Circumstance from the ETC. (Attachment B)

Certification Processes

Election systems manufacturers continually conduct new product development to enhance current voting equipment and innovate the next generation of voting technology. This development process is driven by state and federal election laws and standards that establish specific voting system requirements.

Software / Firmware

After internal vendor development, documentation, and quality assurance, to be certified to federal voting systems standards, a voting system and its component parts must go through extensive testing conducted by EAC accredited Voting System Testing Laboratories (VSTL). VSTL's review line-by-line the software and firmware source code to ensure compliance with standards and overall integrity. Once complete, a VSTL will perform and witness the compilation of the source code into program executable files. VSTL's test the functionality of the voting equipment using compiled code to ensure it operates accurately - that votes are properly captured, results are properly reported, and data is properly retained. To pass the accuracy test, a system must tabulate 1.5 million votes with 100% accuracy.

Voting System Hardware

VSTL's test the operation of the voting system hardware to ensure it can withstand extreme environmental conditions and intensive human handling. If, at any point in the testing process, a VSTL identifies an issue that must be addressed, a product or component part is sent back to the vendor for additional development and resubmission through the whole VSTL testing process. Only after the system or component has passed every test is it deemed qualified for federal certification.

State-level Certification

Presently ~thirty-six states (36), federal certification is only a first step before a voting system can achieve state certification. In many cases, the state will carry out its own independent testing of the accuracy, security, and reliability of a system. State testing (which varies state-to-state) expands upon and enhances testing at the federal level. A state also will compare a product's features and functionality against state law and standards to ensure it complies. Many states require the vendor to escrow a copy of the certified system software.

Local Jurisdiction

Locally, after vendor production testing prior to shipping, the local election authorities conduct acceptance testing to ensure the voting system equipment

performs properly and has met state and federal level certification. Further still, prior to every election, local election authorities perform logic and accuracy (L&A) tests of the voting system and procedures with election-specific ballots to confirm it functions properly and is secure. And in many jurisdictions they perform a pre-advertised public test of the voting system.

To learn and understand more about the multiple steps within the Certification process, please see the attached document (Attachment C: Current certification processes) which shows the VSTL Review Process. Also, from the ETC is a document graphically showing the Testing and Certification process prior to November 2005. (Attachment D: Previous certification process)

Source Code Analysis

During the federal and state level certification process, authorized reviewers have full access to the voting system source code and reports of system performance. During each subsequent certification event the source code is re-reviewed against prior versions.

To enhance the transparency of source code, ETC member companies support and embrace the development, by the Election Assistance Commission, of a program designed to allow qualified reviewers an opportunity to review the source code of the manufacturer's proprietary software. This review should be conducted under an established set of rules and regulations designed to ensure security of voting systems while also protecting vendors from copyright infringement.

Source code is currently provided or "disclosed" in a number of ways. First, the EAC also requires that the executable software compiled from the certified source be submitted to the National Institute of Standards and Technology (NIST) for the generation and public posting of digital signatures ("hash codes").[1] Jurisdictions can use these hash codes in performing tests on the voting system software to verify that they have the correct version of certified software.

Secondly, the source code is provided to the Voting System Testing Laboratories (who are accredited by the EAC) for use in testing and certifying voting systems. ~Thirty-six (36) states also require the manufacturer's source code as part of their certification and review process; in every instance that source code is provided. Customers and/or states may also require the manufacturer's source code be escrowed with the code being provided under escrow agreements.

Also, after software is federally certified, election system vendors voluntarily submit the executable code to the National Software Reference Library, which archives a validation code for future reference. This allows any jurisdiction to verify the delivered system software against the archived validation code to ensure it is the certified version.

The ETC members believe that a good process for disclosed source would be like the attached the testimony concerning the Open Source Software debate from election expert Britain Williams, Ph.D. Dr. Williams is Professor Emeritus, Kennesaw State University whom has more than 20 years experience in computer based training. Dr. Williams's testimony is from the Election Subcommittee Hearing on Election Reform on March 15, 2007. (See attachment E)

Concluding Remarks:

In providing this testimony, our intention is to give feedback to the Subcommittee of Information Policy, Census, and National Archives, Committee on Oversight and Government Reform on the consequences to the vendor community and, as we see it, to the states and election jurisdictions – our valued customers whom we serve.

Above all, the ETC member companies and employees aim to be responsive to voters, local election officials, State and Federal government, and is committed to providing safe, secure, accurate, reliable and accessible voting systems. We are all involved in this process together, and by working together we can improve the process of voting, voter access and participation.