

Computer Security Experts Support BC-LCCR Recommendations

“Members of the National Committee for Voting Integrity (NCVI), would like to commend the Leadership Conference on Civil Rights and the Brennan Center for Justice at NYU School of Law for your efforts to increase awareness among election administrators on methods for addressing many concerns communicated by computer security experts regarding currently available direct recording electronic (DRE) voting technology. Your recommendation to Election Officials that they request that companies make their underlying software code for electronic voting technology available for inspection is the first step that our committee has outlined as being key to restoring trust in public elections. The NCVI will continue to work for a comprehensive security review of all voting technology to fully resolve all security issues so that our nation's election system will truly be the envy of the free world.”

The National Committee for Voting Integrity (NCVI) brings together experts on voting issues from across the country to promote constructive dialogue among computer scientists, elections administrators, policymakers, the media and the public on the best methods for achieving a voter verified balloting system. In keeping with the goal of public election administration, election systems must preserve vote accuracy; insure privacy, and the proper tabulation of the voter's intent regardless of his or her physical condition, language of origin, or literacy ability. <http://www.votingintegrity.org/>

*Committee Members: Peter G. Neumann, Chair * David Burnham * David Chaum * Cindy Cohn * Lillie Coney * David L. Dill * David Jefferson * Jackie Kane * Douglas W. Jones * Stanley A. Klein * Vincent J. Lipsio * Rebecca T. Mercuri * Justin Moore * Jamin Raskin * Marc Rotenberg * Avi Rubin * Bruce Schneier * Paul M. Schwartz * Barbara Simons * Sam Smith*

“EPIC is pleased to endorse the Leadership Conference on Civil Rights and the Brennan Center recommendations being made today to Election Administrators throughout the Nation. This document provides important guidance to them on ways that they could positively address some of the identified security problems associated with paperless DRE voting technology. We believe that these recommendations if implemented aggressively present an opportunity for Election Administrators to bring accountability to their advocacy of meaningful voting rights in their jurisdictions. Over a year ago, EPIC began an effort to improve awareness about the lack of transparency of newly deployed DRE voting technology (<http://www.epic.org/privacy/voting/>). That effort culminated in the creation of the National Committee for Voting Integrity (NCVI) (<http://www.votingintegrity.org/>), which will continue to work with the LCCR and the Brennan Center in its efforts to improve our nation's voting system not just for the November 2004 Election, but into the future. EPIC's commitment to privacy and transparency for every voter forges our resolve to achieve equal access for all eligible voters to participate public elections.”

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., which has recently celebrated its 10th Year of Service to the Privacy Interest Community. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.

"The BC-LCCR recommendations could go a long way towards increasing confidence in the results of the 2004 elections. I call upon all election officials to pay close attention to these recommendations and implement them as quickly and comprehensively as possible."

David L. Dill, Professor of Computer Science, Stanford University.

"Free and open voting is one of the most essential foundations of our system of a democratic society. It is because of that, the integrity of our voting process MUST insure that election officials take to the proper measures to reduce the risk of voting system failures and security breaches. Voting rights experts and election officials, working closely with the technology and computer security community, need to co-develop concrete recommendations that can meaningfully improve voting security. It is imperative that we do everything that we can to protect the integrity of the all future elections by using this Brennan Center report as a starting point to build on for an electronic voting system that is accessible and secure for all citizens."

Howard A. Schmidt, Former Cyber Security Advisory White House, formerly Director of the U.S. Air Force Office of Special Investigations (focusing on, among other things, Computer Crime and Information Warfare) and chief security officer at Microsoft.

"Elections require an end-to-end concern for a wide variety of integrity requirements, beginning with the registration process and ballot construction, and continuing through vote tabulation and reporting. The LCCR / Brennan Center for Justice recommendations represent some very important measures that would significantly improve the overall election process, although they cannot by themselves ensure the integrity of today's un-auditable all-electronic systems -- with which errors and intentional alterations of software and results can easily go completely undetected. The National Committee for Voter Integrity (<http://www.votingintegrity.org>) and I look forward to working jointly with civil-rights, voting rights, and disability advocacy communities to improve election integrity for all voters, by November 2004 to the extent possible. We are committed to working with these groups in the long term toward a non-discriminatory voting system with high-integrity and full accountability, which would make public elections accessible for all."

Peter G. Neumann, Principal Scientist, SRI International's Computer Science Laboratory; Fellow of the AAAS, ACM, and IEEE; and recipient of the ACM Outstanding Contribution Award in 1992 the Electronic Frontier Foundation Pioneer Award in 1996, and the ACM SIGSOFT Outstanding Contribution Award in 1997.

"With only several months to go before the election, the best way to address the current crisis in voting for 2004 is to bring in security experts with a mandate to discover the problems and find practical ways to mitigate the risks. The LCCR / Brennan Center for Justice recommendations explain specifically how to go about this process and supply a model RFP to speed the work of the states. Election officials should move forward rapidly. For 2006 and on, there is much that can be done to build high-confidence, verifiable voting systems which have accessibility for disabled people as well as people with limited English proficiency."

Avi Rubin, first author of the much noted Hopkins' study of DRE voting machines, Technical Director, Johns Hopkins University Information Security Institute, Professor,

Johns Hopkins University, formerly of AT&T Labs - Research, Secure Systems Research Department and Bellcore, Cryptography and Network Security Research Group.

“It is essential for states and local jurisdictions to face the hard questions posed by the election technology they are using, and to do so quickly. Voters must be assured that the weaknesses of current voting systems are addressed by the procedures used to administer this fall's general election. The LCCR / Brennan Center for Justice recommendations for 2004 make a big contribution to this and should be implemented immediately by election officials who expect to use direct-recording electronic voting systems this November.”

Douglas W. Jones, associate professor of computer science at the University of Iowa, has served on Iowa's Board of Examiners for Voting Machines and Electronic Voting Systems for the last decade, is a member of the National Committee for Voting Integrity, vice president and chief technical officer of the Open Voting Consortium, and has testified before the United States Civil Rights Commission, the House Science Committee and the Federal Election Commission on voting technology issues.

“Much can be done to address the critical problems with our voting systems in 2004. These LCCR / Brennan Center for Justice recommendations are essential. After this election, we should move to the next step, both technologists and civil rights advocates together with others and create voting systems we can fully trust. I see this joint effort of the LCCR / Brennan Center for Justice team as a first step in this critical direction.”

Bruce Schneier is the founder and CTO of Counterpane Internet Security, Inc., a premier provider of Managed Security Monitoring services, cryptographer and respected author of many works about computer security related issues and winner of the Secure Computing Lifetime Achievement Award from Secure Computing Magazine in 2003.

“Integrity of voting is critical to public confidence in government. The Brennan Center For Justice / Leadership Conference on Civil Rights recommendations supply elections officials with the steps for improving the quality of elections. Secretaries of state not lose any time moving forward.”

Bill Inmon, Founder, Inmon Data Systems, Inc.

“Since the very integrity of the November election rests on electronic voting machines with well known and potentially easily exploitable security problems, short cuts are not appropriate. It is only prudent for each jurisdiction to assess the security of its particular electronic voting machines and the effectiveness of its procedural controls. The Brennan Center For Justice / Leadership Conference on Civil Rights recommendations supply elections officials with the steps for doing this.”

Jonathan G. Gossels is President of SystemExperts Corporation, a consulting firm specializing in network security and system management. He plays an active, hands-on role advising clients in technology strategies, managing complex programs, and resolving organizational issues related to technology initiatives.

“Putting high-quality security reviews of voting systems in place is a very good idea.”

Ronald L. Rivest, Andrew and Erna Viterbi Professor of Electrical Engineering and Computer Science in MIT's Department of Electrical Engineering and Computer Science, co-investor of a key technology used worldwide to permit e-commerce on the internet (the RSA public key encryption technology), founder of RSA Data Security.

“The rapid growth of new technologies to more accurately and faithfully record our votes has opened up a Pandora's box of concerns that fester in the absence of guidelines for the building and testing of these systems. The LCCR / Brennan Center For Justice recommendations are an essential first step toward meeting these needs. I'm looking forward to working closely with the civil rights community to move toward secure and accessible voting systems for 2006 and thereafter.”

Michael Wertheimer, RABA Technologies. Dr. Michael Wertheimer recently completed a twenty-one year career as a mathematician at the National Security Agency where he worked to defend our nation's most critical communications. He is now Director of RABA Technologies Innovative Solution Cell for which he led a study of Maryland's electronic voting system. He has testified to the Maryland and Ohio legislatures on his team's findings and authored several articles on electronic voting.

“The LCCR / Brennan Center for Justice recommendations are an important milestone in ensuring the integrity of our nation's new election systems. Given that approximately 29% of the electorate this November will cast their votes using paperless direct recording electronic (DRE) systems, it is critical that these DRE systems and the policies and procedures involved in handling them be subject to critical and unbiased scrutiny. The current ‘certification’ system has proven to be far too lenient, raising important and unanswered questions about the integrity of our elections. Our election officials need to adopt these recommendations quickly and move aggressively to study and improve the systems we will be using on Election Day and beyond.”

Dan Wallach, assistant professor in the systems group at Rice University's Department of Computer Science. Dr. Wallach studies computer security, including mobile code security, peer-to-peer networking security, wireless security, and voting systems.

“Direct-recording electronic voting systems have been shown to contain numerous security flaws. Election officials who plan to use them for this fall's general election should ensure that election procedures limit the possibility of exploitation of these flaws. In particular, the kind of careful review proposed in the LCCR/ Brennan Center for Justice recommendations for 2004 is critical.”

Rahul Simha, Associate Professor of Computer Science, received his PhD in 1990 from the University of Massachusetts, Amherst. His research interests include computer systems, embedded systems and security.

Jonathan Stanton is an Assistant Professor of Computer Science at the George Washington University. His research is in secure networked systems and he co-founded a company focused on highly reliable and dependable distributed systems.

Poorvi Vora, Assistant Professor of Computer Science at the George Washington University, was Security Architect in the Office of the CTO of Printing and Imaging at Hewlett-Packard before GW. Her interests are in cryptology and privacy.

“I see the training component of the LCCR/BC Recommendations as most important. If poll workers are not well trained, then inaccuracy is just a forgone conclusion.”

Alan Dechert has been a software test engineer and application developer for the past 15 years. In 2003, along with Dr. Douglas W. Jones (Univ. of Iowa) and Dr. Arthur Keller (UC Santa Cruz), he founded the Open Voting Consortium (OVC). He currently serves as President and CEO of the OVC.

“The report’s proposal -- given today’s diminished voter confidence, poor performance of many DRE’s and the inherent weakness of their trusted voting machine concept -- goes a long way towards engendering an atmosphere of appropriate diligence that may turn around those who otherwise would be disenfranchised through their own skepticism. The details of the report are also particularly to be commended for providing a clearly articulated and actionable program that can accommodate the different legal, procedural, and technical situations in the various states.”

David Chaum is a well-respected cryptographer and widely recognized as the inventor of eCash and founder of its pioneering company DigiCash. Chaum has also proposed a number of much cited promising techniques for secure secret-ballot elections.

“Security is a process and these recommendations are an important step in the direction of improving election security for November. It is critical that these recommendations be implemented and the results widely publicized so that voters will be more motivated to exercise their democratic rights.”

Moti Yung, inventor of many crypto technologies including pioneering cryptographic election protocols.

“The recommendations of the LCCR and the Brennan Center can dramatically improve the reliability and security of the November, 2004 election. I would hope these recommendations would be quickly implemented everywhere that electronic voting machines are used. There is no time to lose.”

David Jefferson, Computer Scientist, Center for Applied Scientific Computing, Lawrence Livermore National Laboratory.

“It is crucial that the 2004 national election be as secure and trustworthy as possible. Given the known problems with paperless electronic voting machines, election officials must be vigilant. The actions outlined in the BC-LCCR recommendations should be on the top of every election official’s to-do list.”

Barbara Simons was President of the Association for Computing Machinery (ACM) from July 1998 until June 2000 and Secretary of the Council of Scientific Society Presidents in 1999. Recently, Simons has been teaching technology policy at Stanford University.

“I thank the LCCR and the Brennan Center for their efforts to provide clear technical recommendations to Election Administrators on methods to improve some of the security problems associated with DRE voting technology in time for the upcoming General Election. It is my hope that these recommendations will be followed aggressively in an effort to restore voter confidence in the election's process. Several members of the National Committee for Voting Integrity (NCVI) made substantial contributions to this effort. Their time and expertise as well as the interest shown by many other member of the NCVI Committee demonstrate their interest in making substantive contributions to improving public election systems. We still have a great deal of work to do in improving our system of public elections, but this is a solid first step in addressing the immediate need of voters to have their security concerns regarding current DRE voting technology addressed.”

Lillie Coney, Senior Policy Analyst with the Electronic Privacy Information Center (EPIC). Her issue areas include, but are not limited to; civil rights, privacy, and electronic voting. Ms. Coney also serves as Coordinator of the recently established National Committee on Voting Integrity (NCVI). NCVI was created in 2003 in response to growing concerns about the reliability of electronic voting systems. Electronic Privacy Information Center.

“These recommendations provide a solid, basic framework for independent investigations into DRE security prior to the November, 2004 elections. They also provide the basic plans for procedural protections and processes to ensure that problems that will inevitably occur do not result in voter disenfranchisement and are properly documented and investigated.”

Cindy Cohn is the Legal Director of the Electronic Frontier Foundation and a member of the Board of Directors of Verified Voting Foundation. EFF provides legal support and representation for scientists who wish to conduct independent investigations into the security of DREs, including the authors of the Johns Hopkins/Rice review of certain portions of the Diebold election system. EFF also assists scientists and activists seeking to strengthen the federal certification processes.