Recommendations of the Brennan Center for Justice and the Leadership Conference on Civil Rights for Improving Reliability of Direct Recording Electronic Voting Systems

Table of Contents

Introduction

Approximately 675 counties across the country – accounting for approximately 30 percent of registered voters in more than half the states – have purchased Direct Recording Electronic ("DRE") voting systems for use in the 2004 elections. Many DRE technologies offer potential advantages of greater accessibility to voters with disabilities and lower rates of lost votes than older technologies, such as punch cards.[1] But concern has grown recently about the vulnerability of DRE systems to security breaches and malfunctions, either of which could result in miscounted votes. In addition, the Chairman of the newly-formed U.S. Election Assistance Commission has indicated that the Commission will consider asking every election jurisdiction that uses such systems to identify and implement enhanced security measures for the 2004 election cycle.

In response to the public controversy about DREs, the Leadership Conference on Civil Rights asked the Brennan Center for Justice at NYU School of Law to undertake an independent assessment of DRE system security and to develop recommendations that could be implemented immediately by jurisdictions planning to use DREs in their 2004 elections. The Center retained a 20-year veteran in the field of technology evaluation, Eric Lazarus of DecisionSmith, to provide the technical assistance with the project. Mr. Lazarus in turn enlisted a team of nationally renowned security experts and consulted closely with others interested in this effort.

In addition to Mr. Lazarus, the team includes Howard Schmidt, formerly Cyber Security Advisor to the White House, 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; Bruce McCulley, a Certified Information Systems Security Professional with extensive experience engineering critical systems; and Dr. Moti Yung, a senior research scientist at Columbia University, and one of the nation's foremost experts in the use of cryptography to prevent information systems attacks, including against voting systems. The recommendation development work was overseen by David Siegel, a noted independent systems consultant with a strong background in transactional and trusted systems especially in finance. Leading experts whom the team has interviewed include, among others, Dr. Michael Wertheimer, Director, RABA Innovative Solutions Cell, who conducted the most comprehensive test of DREs for potential errors and security breaches completed to date; Dr. Douglas Jones, professor of computer science at the University of Iowa, and one of the foremost computer voting technology experts in the country; Dr. Ted Selker, an MIT professor who directs the Media Lab's Context-Aware Computing group; and two inventors of cryptography-based voting systems, David Chaum and Jim Adler.

---

[1] *See, e.g.*, David C. Kimball, *Voting Methods Two Years After Florida*, July 2003 (on file with the Brennan Center) (concluding that non-full-face-ballot DRE voting systems significantly reduce the number of unrecorded votes in top-of-the-ballot contests); League of Women Voters, *Questions and Answers on Direct Recording Electronic (DRE) Voting Systems and the Proposal to Require a Voter-Verified Paper Trail (VVPT)*, available at http://www.lwv.org/join/elections/HAVA_QAonDRE.pdf.

Team members conducted an extensive review of the literature (print and electronic) on DRE security, interviewed experts throughout the nation, developed preliminary assessments of the arguments for and against DREs, and discussed their results extensively with Brennan Center attorneys. Through this effort, the team developed the following recommendations for jurisdictions that plan to use such DRE systems in 2004. If implemented by those jurisdictions within the obvious constraints of time and resources, these recommendations can markedly improve confidence that such DRE voting systems will function properly on Election Day and that votes will be recorded and counted correctly.

Our 2004 recommendations, presented below, are offered with two assumptions in mind. First, we assume for purposes of our analysis that the target jurisdictions own certified DRE voting systems that will be used in the 2004 fall elections. Accordingly, these recommendations should not be seen as an endorsement or indictment of such systems or their use. A full analysis of the benefits and pitfalls of DREs and other voting systems remains necessary but is outside the scope of this report. Second, these recommendations are intended for immediate implementation over a short period of a few months and thus are limited in scope. If implemented in full, however, these recommendations will help to alleviate certain risks of security breaches and machine malfunctions and to improve public confidence in the election administration in the target jurisdictions. Privacy and transparency are key components of a free and democratic system of government. For this reason, it is important for voting technology, which is intended for use in public elections, to be transparent. Independent review of voting system technology can achieve some measure of transparency of the election process. We consider these recommendations to be minimum essential steps to achieve all of these ends.

We recognize, of course, that voting systems other than DREs are susceptible to operational failure or malicious attack. Some have relatively high rates of failure. Regardless of the technology used, votes may not be counted accurately unless machines function correctly and elections officials and poll workers are thoroughly trained and properly supervised in the set-up, use, care, and protection of a jurisdiction's voting system. In other words, all voting systems stand to benefit from an assessment of the sort provided for DREs here. But that comprehensive analysis is beyond the scope of this initial report.

Recommendations

This report recommends that elections officials in jurisdictions planning to use DRE voting systems in the fall 2004 elections take action in several key areas to assess and address potential vulnerabilities in their voting systems.

1. Elections officials should hire a well-qualified, independent security team to examine the potential for operational failures of and malicious attacks against the jurisdiction's DRE voting system.

2. The assessment performed by the independent experts should cover at least following areas of concern:
    a. Hardware Design
    b. Hardware/Firmware Configuration
    c. Software Design
    d. Software Configuration
    e. Election Procedures
    f. Physical Security
3. Elections officials should implement the critical recommendations of the independent expert security team and demonstrate to experts and voters alike that the recommendations have been implemented.
4. Elections officials should provide a thorough training program for all elections officials and workers on security procedures to ensure that security procedures, including those recommended by the independent expert security team, are followed even in the face of Election-Day exigencies.
5. Elections officials should develop procedures for random parallel testing of the voting systems in use to detect malicious code or bugs in the software.
6. Elections officials should have in place a permanent independent technology panel, including both experts in voting systems and computer security and citizens representing the diverse constituencies involved in election oversight, to serve as a public monitor over the entire process outlined above and to perform a post-election security and performance assessment.
7. Elections officials should establish standard procedures for regular reviews of audit facilities and operating logs for voting terminals and canvassing systems to verify correct operation and uncover any evidence of potential security breaches.
8. All jurisdictions should prepare and follow standardized procedures for response to alleged or actual security incidents that include standardized reporting and publication.

The following sections address each of these recommendations in greater depth.

1. Retaining Independent Security Experts

After widespread reports of alleged flaws in voting systems manufactured by Diebold, Inc., Maryland officials retained independent experts on two occasions to assess the "threats, vulnerabilities, security controls, and risks associated with the AccuVote-TS system [manufactured and sold by Diebold to Maryland] and possible impacts to the State and the integrity of its elections process from successful exploitation of identified

weaknesses."[2] The risk assessment prepared by Science Applications International Corporation, and the more in-depth technical analysis by RABA Technologies, provide important precedents and valuable lessons for elections officials concerned about DRE voting system security. Similarly, Ohio elections officials retained two firms, InfoSENTRY and Compuware, to undertake studies that yielded similar reports and recommendations.

To begin, these precedents demonstrate the importance of retaining an independent firm with deep and broad expertise in computer security, rather than relying upon either assurances from a vendor or in-house expertise. In order to perform the necessary analysis and ensure public confidence in that analysis, the expert security team that is retained must be free of any business relationships with any voting system vendors or designers. The outside team must also have a proven track record in assessing computer security in voting systems or comparable technologies.

Further, the independent expert security team must be allowed full access to the hardware/firmware, software code, procedural protocols, design documentation, and other relevant items associated with the DRE voting system under analysis.[3] With growing pressure from voters and public officials to provide voter-verifiable paper trails, DRE system vendors should be willing to allow such access, because refusal may result in de-certification of their systems.[4] To ensure such access, however, elections officials

---

[2] Science Applications International Corporation, *Risk Assessment Report Diebold AccuVote-TS Voting System and Processes*, at III (Sept. 2, 2003), available at http://www.dbm.maryland.gov/dbm_search/technology/toc_voting_system_report/votingsystemreportfinal.pdf. The Maryland Department of Budget and Management's Office of Information Technology commissioned Science Applications International Corporation ("SAIC") to prepare what became SAIC's September 2, 2003 report. Subsequently, the Maryland Department of Legislative Services commissioned RABA Technologies, Inc. to prepare further analysis, which appeared in a January 20, 2004 report.

[3] It is essential that the independent expert team has complete access to all of the source code for all software running on both the DRE devices themselves and on the back-end canvass systems. All of the logic for conducting the election resides in that software, and most of the work in certifying DREs consists of examining that software for security, reliability, functionality, accuracy, usability, manageability, capacity, and a variety of other software properties, along with conformance to state election laws. In addition, the expert team requires copies of all software design documents and other documentation to aid in navigation through the source code, as well as complete documentation of how the source is converted to the object code (*e.g.*, details about compilers, compiler options used, libraries, configuration parameters, etc.). It is also essential to have a version history and change log of the software; information on the status of known outstanding bugs, security vulnerabilities or other limitations; test data and programs suites; and regression protocols. All of this information should be provided, subject to appropriate confidentiality agreements, to elections officials and the expert team that is retained. Recently, the Chairman of the U.S. Election Assistance Commission indicated publicly that the Commission intends to consider requesting that all voting system software vendors allow elections officials full access to proprietary software codes with appropriate confidentiality agreements. *See* Chairman Soaries' Remarks about Electronic Voting Security Strategy for the November 2004 Presidential Election (on file with the Brennan Center).

[4] In April, California's Secretary of State decertified certain DRE voting systems across the state as a result of security concerns over Diebold DRE systems used in the March presidential primary election. *See* Kim Zetter, *California Bans E-Vote Machines*, Wired, April 30, 2004, available at http://www.wired.com/news/evote/0,2645,63298,00.html. The Secretary of State's report is available at http://www.ss.ca.gov/elections/ks_dre_papers/decert1.pdf.

from the various states that have purchased the same vendor's systems should collectively demand full and complete cooperation from the vendors to facilitate independent risk assessments. In addition, they should inform vendors that their level of cooperation will be documented on publicly visible websites for purchasers including secretaries of state to review. Where possible, contract terms may be used to require such cooperation (and future state purchase contracts should be drafted to include such requirements). Such alliances of state elections officials could also be used, where appropriate, to take advantage of economies of scale in the assessments themselves. While many of the most important elements of a voting system are the site-specific procedures for using the machines on or before Election Day, certain elements of hardware and software design and configuration are plainly common to a single vendor's system, irrespective of the jurisdiction in which it is used. In the absence of federally sponsored in-depth security assessments of specific voting systems, such multi-state alliances may provide fruitful opportunities to enhance voting machine security on an expedited basis. This may be particularly valuable to avoid duplicative assessments of identical voting system technologies used in different jurisdictions. Indeed, once a full assessment of a given voting system has been completed and can be shared among all jurisdictions that use identical technology (*i.e.*, hardware and software), elections officials and the independent experts with whom they contract should be able to focus more exclusively upon those elements that are unique to their jurisdiction.

2. Performing Voting System Assessment

The expert security team that is chosen should include within their scope of work and final recommendations, at a minimum, the analyses listed below.[5] Each jurisdiction and each voting system will inevitably present unique concerns that must be assessed by the contracting expert security team. Indeed, officials should establish that one of the most important aspects of an expert security team's preliminary review will be to identify areas of vulnerability that are unique to the jurisdiction at issue. In addition, as noted already, elections officials can and should take advantage of voting system assessments performed in other jurisdictions on identical hardware and software systems.

a. Hardware Design Assessment

Potential vulnerabilities: Hardware design flaws can allow an attacker to access the voting system to change critical settings, install malicious devices, or otherwise tamper with the voting terminals or tally servers. Examples include machines or ancillary components without sufficient locks, with exposed drives, or with other easily accessible hardware components. Such vulnerabilities could lead to machine malfunctions, miscounted votes, or erasure of data, were an attacker able to exploit them.

[5] Elections officials should consult the procedures described in the publication NIST 800-30, "Risk Management Guide for Information Technology Systems" and the baseline information categories defined in the NSA Infosec Assessment Methodology. These documents are used by the U.S. Government to define the scope of work for its security assessments.

Recommendations: In the area of hardware design, a critical assessment tool has been so-called "red team" exercises, in which a team of analysts attempts to attack the system under review to identify points of vulnerability.[6] In addition, the hardware must be studied to identify design flaws that could allow either access to attackers or mere operational failures. All devices and casings must be protected against such access. The independent expert security team should provide a comprehensive assessment of hardware design flaws or opportunities for improvement.

Among other remedial recommendations that have resulted from such hardware design assessments are: the use of "tamper tape" on vulnerable hardware components to ensure that attempts to breach those components are detectable, replacement of certain hardware components with less vulnerability, and new security procedures to compensate for an identified hardware design flaw.

b. Hardware/Firmware Configuration Assessment

Potential vulnerabilities: Hardware or firmware configuration refers to the manner in which different hardware or firmware components are connected and their operating settings.[7] Certain configurations create more potential access points through which malicious attackers could gain access into the voting system. Examples include the ability to "boot" a voting terminal or tally server from a diskette or CD ROM (rather than from an internal hard drive) and thereby gain access to the software code of that terminal or server without a password. Such vulnerabilities could allow an attacker to cause significant damage, from systematically erasing or misrecording votes as they are cast to complete machine malfunctions.

Recommendations: "Red team" exercises and other tools should be used to assess the vulnerability within hardware/firmware configurations in the DRE voting system. All devices must be checked to ensure that proper locks with unique keys or passwords are used; network access is not available through modems, Ethernet ports, or other points between or in hardware components; and machines can be booted only off a secure drive (as opposed to a CD ROM or floppy disk).

---

[6] As described in RABA's report, "A Red Team exercise is designed to simulate the environment of an actual event, using the same equipment and procedures of the system to be evaluated. Teams are then free to experiment with attack scenarios without penalty." RABA Technologies LLC, *Trusted Agent Report Diebold AccuVote-TS Voting System*, at 16 (Jan. 20, 2004), available at http://mlis.state.md.us/Other/voting_system/trusted_agent_report.pdf. RABA's red team exercises focused on smart card vulnerabilities, the security of each voting machine terminal and of the server, and the methods used to upload results after an election. *Id*.

[7] Firmware commonly refers to the coded instructions that are stored permanently in the read-only memory ("ROM") inside a computer system's hardware. It is thus easier to change than hardware but harder than software stored on a disk. Firmware is often responsible for the behavior of a computer system when it is first switched on. A typical example would be a firmware program that loads an operating system from a hard drive or from a network and then passes control to that operating system once the computer is fully booted.

Among other recommendations that are likely to address such concerns are configuration controls, so that it is not possible to boot off a CD ROM or floppy disk; the use of user names, passwords, and file access controls that are unique and inaccessible to potential attackers; and the use of "tamper tape" to protect the server or voting terminal from tampering.

c. Software Design Assessment

Potential vulnerabilities: Software design vulnerabilities could involve either good faith flaws or malicious software code hidden within the voting system. Examples of good faith design flaws include poor practices, such as including passwords or encryption keys in lines of easily accessible software,[8] or simply faulty software code that leads to voting machine malfunctions on Election Day. Malicious software code could include instructions to a voting system to count votes erroneously at random or in specified patterns designed to affect the tallies of a voting machine or an entire election. Although computer security experts warn that it is virtually impossible to guarantee that malicious code has not been introduced into a system, certain basic measures can be taken to reduce the risk of bad software design substantially, whether of unintentional or malevolent origins.

Recommendations: To assess the vulnerability of the system's software, the independent expert security team should review source code with particular attention to authentication, encryption, and the accessibility of critical files, such as those containing voting records. In short, the expert security team must assess the extent to which the source code itself includes unnecessary security risks that could be reduced through patches, encryption, or other security measures, and whether the source code follows good engineering practices to reduce the risk of accidental failures.

In addition to security risks, the expert security team should perform extensive tests of the basic functionality of each aspect of the voting systems, including the recording and reporting of votes. Such testing is essential to assure good software quality. Although it is virtually impossible to guarantee that even an expert will find cleverly written malicious software code, extensive testing will increase the likelihood that the product of such code will be detected before Election Day.

Among other recommendations that are likely to address software design problems are: specific updated patches; crypto-signatures (*i.e.*, digital "fingerprints") to ensure that any unintended software code can be identified more easily; and, in the case of good faith software design flaws, revisions to software source code to address specific problems of security or functionality. Note that such revisions must themselves undergo security assessments, within the constraints of time, before use on Election Day.

---

[8] *See, e.g.*, RABA Technologies LLC, *supra* note 6, at 16. RABA's red team exercises revealed that the smart cards' passwords were actually contained in the source code for the systems, which allowed the team easily to gain access to a card's contents and thus to vote multiple times.

d. Software Configuration Assessment

Potential vulnerabilities: Software configuration refers to the ways in which the various software elements are set up and arranged together to work properly. Flaws in such configuration can allow unintended access into the software code by an attacker, or simply expose the software to common dangers, such as computer viruses. Examples of vulnerable software configurations include the failure to ensure that anti-virus software programs or other software "patches" designed to block unauthorized access are in place and up-to-date throughout the system.[9] In addition, the software configuration could also expose weak links in the security of the connections between various software components, through which an attacker could gain access to the system and affect the machines' operation.[10] Uncertainty about poorly controlled configuration details will make security assessment much more difficult, if not impossible.

Recommendations: To assess software configuration problems, the independent expert security team should analyze the entire voting system to examine how data flows from one element to another. For example, experts may find that there is a security vulnerability in the software that moves the ballot information into the vote capture system to record the vote. Each separate device or interface between devices (and the software inside) represents a potential point of attack that must be assessed. In addition, experts must examine the patches and anti-virus software used in the servers and the terminals. Further, the expert security team should study the procedures and mechanism, if any, to upgrade software in the system. To assess whether improper software upgrades have occurred, the expert security team must compare the existing code with the most trusted version of the same. If software upgrades are to be completed from a remote location, the risks inherent in such upgrades must be documented and assessed. In any event, software upgrades and even parameter changes should be carefully controlled and documented at all times, and the procedures for doing so should be reviewed as part of the assessment process.

Among other recommendations that are likely to address software configuration problems are: placing digital signatures on software to detect malicious code, precluding any remote software upgrades as unacceptable risks, new patches in the operating systems to improve security, and reconfiguration of certain software elements to eliminate weak links in the system.

---

[9] For example, the RABA investigators who analyzed the Diebold machines to be used in Maryland found that, with the correct phone number of the central server in each local board of elections, they could take control of the entire server from any phone in the world. The vulnerability was the result of failure to update the so-called "GEM Server" with at least 15 security patches available from Microsoft. *Id*. at 20-21.

[10] The *Seattle Times* reports that an internal Diebold email allegedly noted that King County (WA) was "famous" for using uncertified Microsoft Access software to open the GEMS election database. *See* Keith Ervin, *No election snags, director says: Absentee ballots on time, security measures in place*, Seattle Times, Oct. 28, 2003, available at http://seattletimes.nwsource.com/html/localnews/2001776406_voting28m.html.

e. Assessment of Procedures

Potential vulnerabilities: The procedures used to handle a voting system can facilitate security breaches or machine malfunctions or, at the least, fail to stop such problems. Examples of problems in this area include the absence of adequate security procedures (*e.g.*, using only one encryption key or password for all machines rather than unique keys or passwords for each machine), poor implementation of adequate procedures by elections workers, or departures from protocol caused by unforeseen circumstances on Election Day.[11] In addition, procedures that are not directly related to security can produce unnecessary security risks. For example, procedures that allow last-minute software upgrades to the machines or server can, if not handled properly, allow uncertified software to be used on Election Day that bypasses critical security safeguards.[12] Inadequate procedures for routine auditing, detection, and response to security incidents can also undermine the effectiveness of other security measures.

Recommendations: To assess both security procedures and election procedures that may have security implications, the independent experts must study relevant procedures in place in the jurisdiction, determine whether they are fully in use, and understand which individuals are trained and responsible to ensure their proper implementation. In addition, the expert security team must assess all locks or other security devices to determine their vulnerability, including such facts as how many keys have been made that can open a lock and to whom the keys have been given. Such analyses must address the entire voting system and must incorporate any changes that occur in procedures on or before Election Day. The objective is to assess the chain of possession from vendor to precinct so that no unintended software modifications or hardware tampering can occur. The same consideration should be given to assessing procedures used to create the chain of possession of voting results, from balloting through certification.

Measures that are likely to improve security and other procedures include: replacement of locks and security devices; implementation or improvement of standard procedures; better training on procedures for key officials and workers; the use of Tripwire, or a similar software authentication program, to provide a check of software

---

[11] The RABA investigators found that all 32,000 of Maryland's touch-screen terminals had the same locks and keys, making every machine accessible to anyone with one of the keys. The keys could also be easily reproduced at three local hardware stores. RABA Technologies LLC, *supra* note 6, at 18. The *Washington Post* reports that malfunctioning machines were removed for repair and returned to service during Election Day in Fairfax County, Virginia. *See* Eric M. Weiss & David Cho, *Glitches Prompt GOP Suit Over Fairfax Tabulations*, Washington Post, Nov. 5, 2003, available at http://www.washingtonpost.com/ac2/wp-dyn/A1397-2003Nov5.

[12] In three central Indiana counties, for example, uncertified firmware was loaded into the voting systems by Election Systems & Software as a result of inadequate procedures. *See* Rick Dawson and Loni Smith McKown, *Voting Machine Company Takes Heat Over Illegal Software*, WISH-TV8, March 11, 2004, available at http://www.wishtv.com/Global/story.asp?S=1704709&nav=0Ra7JXq2. In California, the installation of uncertified software occurred on several occasions and led to the Secretary of State's decertification of DREs. *See, e.g.*, Kim Zetter, *E-Voting Undermined By Sloppiness*, Wired, Dec. 17, 2003, available at http://www.wired.com/news/evote/0%2C2645%2C61637%2C00.html.

integrity on the machines and server; and protocols for use of "tamper tape" and other protective measures.

f. Physical Security Assessment

Potential vulnerabilities: Voting systems must be securely stored and kept physically out of the reach of potential attackers. Without such physical security precautions, the finest security checks on voting terminals or servers may be rendered moot by subsequent attacks on or before Election Day, software or hardware may be maliciously altered, and machines may be programmed to miscount or erase votes or simply to malfunction in certain areas or polling places.

Recommendations: The assessment of physical security will require different analyses in different jurisdictions, depending upon the size of the jurisdiction, the number of machines, the methods of storing and handling the machines, and other factors. The independent expert security team must study the entire chain of custody of all of the voting terminals, the servers, and any other materials related to the use of the DRE voting systems. The "chain of custody" assessment should also cover the recording and transmission of voting results, including all telecommunications or networking facilities utilized. The chain of custody must not end on Election Day, moreover, in case of the need for a new election or additional analysis of the systems after the election.

Among other recommendations that are likely to address physical security concerns are: changes in storage methods for machines and servers, limits on personnel access to such components, improved security procedures, and better training of election workers to avoid unnecessary exposure of voting system components.

3. Implementing Expert Recommendations

Eliminating unnecessary security risks and restoring public confidence in voting systems within a jurisdiction requires not just obtaining a risk assessment but also implementing measures to limit those risks before Election Day. For this reason, elections officials should commit prior to hiring an independent expert security team to implement all reasonable recommendations within a pre-established timetable and to provide public explanations (working in concert with the independent oversight panel) of any decisions not to implement specific recommendations. Officials should provide public notice of both the risk assessment process and the plan for implementation of such recommendations. The independent oversight panel recommended below would be a valuable asset in this effort.

In addition, the independent expert security team should be required to identify a series of checks that can be performed after the recommendations have been adopted and implemented that will test whether they have, in fact, been so implemented. Such tests are critical not only to ensure that security and operational improvements have been

made, but also to instill public confidence that the independent assessment process was indeed independent.

4. Developing Security Training

Any serious expert assessment will result in recommended improvements in the training of elections officials and workers to address security concerns and operational failures on DRE voting systems. This is true because experience with DRE machines is still limited in most jurisdictions, and election worker training often remains limited in any event. Accordingly, elections officials should develop a comprehensive security training program for election workers at every stage in the election process. Although the specifics of each jurisdiction's training will differ, all jurisdictions must include training on the changes implemented in response to the independent expert security team's recommendations.

5. Randomized Parallel Testing

Parallel testing is the only procedure available to detect non-routine code bugs or malicious code on DRE systems. In addition to laboratory testing during the certification process it is essential that DRE systems get tested *during real elections*, using so-called parallel testing procedures. Parallel testing is needed for two separate purposes: (a) to test the myriad parts of the system that get used during a real election but not in a laboratory testing situation, and (b) to check for the possible presence of malicious code or insider manipulation that is designed specifically to avoid detection in a laboratory or testing situation, but to modify votes surreptitiously during a real election. Where possible, parallel testing should be performed in every jurisdiction, for each distinct kind of DRE system. While experts agree that parallel testing cannot reveal all forms of malicious code, it can be a critical part of the kind of comprehensive security measures recommended in this report.

Parallel testing involves selecting a *random* sample of the DREs to be used in the election, and setting them up in mock precincts. Then, using all of the same procedures and during the same hours as the real election, mock elections are conducted in the mock precincts. Two separate mock elections should be conducted, one with real volunteer voters, and one with trained personnel following a voting script that represents as accurately as possible the statistical voting profile of a precinct in the county. The entire process, and in particular what happens on the DREs' screens, should be videotaped. At the end of the day, after the mock precincts have been closed down, the mock election results must be reconciled with what the videotape shows that the results should have been.

6. Appointing Independent Security Oversight Panel

Officials should have in place a panel that includes experts in computer security and voting technologies, as well as citizen groups representing the diverse constituencies within the jurisdiction, to perform two key functions. First, such a panel should act as a watchdog to oversee the entire assessment process and implementation of the independent expert security team's recommendations. Public confirmation by such panel that the process provided a truly independent review and that elections officials properly implemented the experts' recommendations would go far in improving public confidence in the near term. Second, the panel should be convened after Election Day to assess the voting system's performance, review the response to any real or alleged security breaches, and evaluate the procedures used on or around Election Day. Based on such post-election assessments, the panel should make its own recommendations to local or state elections officials to address any concerns with regard to the DRE voting systems in use, monitor ongoing efforts to improve voting systems, and bolster public confidence in the election process.

Ideally, such independent oversight panels will be established in state or local laws and will be consulted when changes in voting systems or software are proposed to address security and other concerns related to the accurate performance of the voting systems in place. Absent legislative action, however, senior elections officials should nevertheless consider appointing such panels on an *ad hoc* basis.

7. Establishing Standard Systems Review Procedures

Elections officials should develop standard procedures for regular inspections of operating logs and all other available audit facilities on all voting system terminals. The IT industry depends upon such procedures as "best practices" because they reveal irregularities and facilitate proper responses.

The review of logs and audit trails should seek to verify that the systems have operated correctly, in conformance with established procedures, and that no unexpected events have occurred. Any evidence of malfunction or potential malicious attack should be regarded as a potential security incident and handled in accordance with established incident response procedures. Ideally, these procedures should be independently reviewed as part of the overall security assessment although schedule constraints may require that they be developed simultaneously with the assessment.

8. Developing Incident Handling Procedures

Standard procedures should be developed and followed to respond to reports of security incidents, alleged or real. Such procedures serve to increase confidence by providing factual information to replace rumor, innuendo, fear, uncertainty, and doubt.

They also serve to protect evidence for investigation and potential prosecution if the worst should happen. Most importantly, they increase confidence and reduce the probability of attacks simply by increasing the probability of detection and identification.

Incident handling procedures will vary according to local jurisdiction, but should include reporting mechanisms, initial response procedures (triage and immediate actions required to preserve evidence while maintaining or restoring poll availability), responsibility and procedures for investigation, and final reporting procedures. It is very likely that some incidents could require that suspect systems be sequestered to preserve evidence; spare units or other back-up systems should thus be readily available. In addition, policies and procedures for counting votes from suspect units and preserving evidence should be determined in advance. Finally, the independent oversight panel recommended above should review all incidents and the associated responses. Incident handling procedures thus should include providing information to the panel to evaluate and use in developing recommendations for future improvements.

Conclusion

The debate about DRE systems has generated much heat. We do not pretend to resolve the controversy with this report. Instead, we seek to shed some light on what can be done to improve the security and reliability of DRE systems that have already been certified and will be used across the country in the 2004 elections. Our analysis suggests that there is much to be done in a very short time. We urge jurisdictions that plan to use DREs to begin immediate implementation of the recommendations described above. Full, expeditious, and open implementation of these recommendations offers the best hope for significantly decreasing risks of security breaches and malfunctions in DRE systems and thereby increasing public confidence that the systems will properly record and report the vote, in the aggregate, on Election Day.