Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	able to transmit fraudulent vote reports to the backend server by dialing in from his own computer. While both the paper trail and data stored on legitimate terminals could be used to compensate for this attack after the fact, it could, at the very least, delay the election results."		encrypted and that the LBE perform a 100% verification of the vote transmissions to PCMCIA cards.
14	*"(The PPP number, username, password, and IP address of the back-end server are also stored in the registry HKEY_LOCAL_MACHINE\Software\GlobalElectionSystems\AccuVote-TS4\ TransferParams. Since the ballot definition may be transported on portable memory cards or floppy disks, the ballot definition may perhaps be easier to obtain from this distribution media rather than from the voting terminal's internal data storage.)"*	M-83, M-89, M-91	Ballots are public knowledge. After the ballot is created at SBE, the LBE performs the Logic and Accuracy tests to ensure validity and correctness.
14	*"We will return to some of these points in Section 5.1, where we show that modifying and viewing ballot definition files does not always require physical access to the terminals on which they are stored."*	M-83, M-91	Modification of the ballot requires access to the PCMCIA cards since the DRE devices are not connected to a network.
15	*"Unlike the other data stored on the voting terminal, both the vote records and the audit logs are encrypted and check summed before being written to the storage device. Unfortunately, neither the encrypting nor the check summing is done securely.* *All of the data on a storage device is encrypted using a single, hard-coded DES [NBS77] key:* *#define DESKEY ((des_key*)"F2654hD4")"*	M-41, M-124	Currently, ~~DES~~ encryption is only used for the resident DRE memory. Once the DRE is powered down, the memory is erased. Note, we have recommended that encryption be employed for the modem transmission of the vote totals. The DRE devices are not connected to a network and physical access would be required to get to the data. The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to connect devices to the system would be easily visible to any of the many election officials.
15	*"Note that this value is not a hex representation of a key. Instead, the bytes in the string "F2654hD4" are fed directly into the DES key scheduler. If the same binary is used on every voting terminal, an attacker with access to the*	M-1, M-5, M-111	Currently, ~~DES~~ encryption is only used for the resident DRE memory. Once the DRE is powered down, the memory is erased. Note, we have recommended that encryption be employed for the modem transmission of the vote totals.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	source code, or even to a single binary image, could learn the key, and thus read and modify voting and auditing records."		employed for the modem transmission of the vote totals. The DRE devices are not connected to a network and physical access would be required to get to the data. The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to connect devices to the system would be easily visible to any of the many election officials.
15	*"Even if proper key management were to be implemented, many problems would still remain. First, DES keys can be recovered by brute force in a very short time period [Gil98]. DES should be replaced with either triple-DES [Sch96] or, preferably, AES [DJ02]."*	M-41, M-124	We found no evidence that data was encrypted. However, the devices are not connected to a network and physical access would be required to get to the data. The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to connect devices to the system would be easily visible to any of the many election officials.
15	*"Second, DES is being used in CBC mode which requires an initialization vector to ensure its security. The implementation here always uses zero for its IV. This is illustrated by the call to DesCBCEncrypt in TSElection/RecordFile.cpp;* *since the second to last argument is NULL, DesCBCEncrypt will use the all-zero IV.* *DesCBCEncrypt((des_c_block*)tmp, (des_c_block*)record.m_Data, totalSize,* *DESKEY, NULL, DES_ENCRYPT);* *This allows an attacker to mount a variety of cryptanalytic attacks on the data."*	M-41, M-124,	Currently, ~~DES~~ encryption is only used for the resident DRE memory. Once the DRE is powered down, the memory is erased. Note, we have recommended that encryption be employed for the modem transmission of the vote totals. The DRE devices are not connected to a network and physical access would be required to get to the data. The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to connect devices to the system would be easily visible to any of the many election officials.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
15	*"Before being encrypted, a 16-bit cyclic redundancy check (CRC) of the plaintext data is computed. This CRC is then stored along with the ciphertext in the file and verified whenever the data is decrypted and read. This process in handled by the ReadRecord and WriteRecord functions in TSElection/ RecordFile.cpp. Since the CRC is an unkeyed, public function, it does not provide any real integrity for the data. In fact, by storing it in an unencrypted form, the purpose of encrypting the data in the first place (leaking no information about the contents of the plaintext) is undermined. A much more secure design would be to first encrypt the data to be stored and then to compute a keyed cryptographic checksum (such as HMAC-SHA1 [BCK96]) of the ciphertext. This cryptographic checksum could then be used to detect any tampering with the plaintexts. Note also that each entry has a timestamp, which will prevent the re-ordering, though not deletion, of records. Each entry in a plaintext audit log is simply a time stamped, informational text string. At the time that the logging occurs, the log can also be printed to an attached printer. If the printer is unplugged, off, or malfunctioning, however, no record will be stored elsewhere to indicate that the failure occurred. The following code from TSElection/Audit.cpp demonstrates that the designers failed to consider these issues:* *if (m_Print && print) {* *CPrinter printer;* *// If failed to open printer then just return.* *CString name = ::GetPrinterPort();* *if (name.Find(_T("\\")) != -1)*	M-41, M-124	Currently, ~~DES~~ encryption is only used for the resident DRE memory. Once the DRE is powered down, the memory is erased. Note, we have recommended that encryption be employed for the modem transmission of the vote totals. The DRE devices are not connected to a network and physical access would be required to get to the data. The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to connect devices to the system would be easily visible to any of the many election officials.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	name = GetParentDir(name) + _T("audit.log"); *if (!printer.Open(name, ::GetPrintReverse(), FALSE))* *::TSMessageBox(_T("Failed to open printer for logging"));* *} else {* *15* *Do the printing: : :}* *If the cable attaching the printer to the terminal is exposed, an attacker could create discrepancies between the printed log and the log stored on the terminal by unplugging the printer (or, by simply cutting the cable)."*		
16	*"An attacker's most likely target will be the voting records, themselves. Each voter's votes are stored as a bit array based on the ordering in the ballot definition file along with other information such as the precinct the voter was in, although no information that can be linked to a voter's identity is included. If the voter has chosen a write-in candidate, this information is also included as an ASCII string. An attacker given access to this file would be able to generate as many fake votes as he or she pleased, and such votes would be indistinguishable from the true votes cast on the terminal."*	M-1, M-5, M-14, O-12, O-14	The devices are not connected to a network and physical access would be required to get to the data. The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to connect devices to the system would be easily visible to any of the many election officials. Additionally, in the State of Maryland implementation, the total votes recorded on the DRE is reconciled with the number of votes cast on the DRE using the paper Voter Authority Card that is placed into the Voter Authority Card envelope, attached to the DRE voting terminal by the election official.
16	*"While the voter's identity is not stored with the votes, each vote is given a serial number. These serial numbers are generated by a linear congruential random number generator (LCG), seeded with static information about the election and voting terminal. No dynamic information, such as the current time, is used.*	T-43	The anonymity of a voter's ballot is preserved because the AccuVote-TS voting system does not use or store personal information and does not provide an individual paper record for each voter, therefore leaving no evidence of a single voter's selections. The individual ballots however, are stored sequentially. If someone kept track of all of the individuals who voted on a particular DRE and then was able to obtain

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	// LCG - Linear Conguential Generator - used to generate ballot serial numbers *// A psuedo-random-sequence generator* *// (per Applied Cryptography, by Bruce Schneier, Wiley, 1996)* *#define LCG_MULTIPLIER 1366* *#define LCG_INCREMENTOR 150889* *#define LCG_PERIOD 714025* *static inline int lcgGenerator(int lastSN)* *{* *return ::mod(((lastSN * LCG_MULTIPLIER) + LCG_INCREMENTOR), LCG_PERIOD);* *}* *While the code's authors apparently decided to use an LCG because it appeared in Applied Cryptography[Sch96], LCG's are far from secure. However, attacking this random number generator is unnecessary for determining the order in which votes were cast: each vote is written to the file sequentially. Thus, if an attacker is able to determine the order in which voters cast their ballots, the results file has a nice list, in the order in which voters used the terminal. A malevolent poll worker, for example, could surreptitiously track the order in which voters use the voting terminals. Later, in collaboration with other attackers who might intercept the poorly encrypted voting records, the exact voting record of each voter could be*		who voted on a particular DRE and then was able to obtain the PCMCIA card, they would be able to tie votes back to individuals. However this would require collusion between multiple individuals.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	reconstructed."		
16	*"Physical access to the voting results may not even be necessary to acquire the voting records, if they are transmitted across the Internet."*	O-23, 0-24	Voting records are not transmitted via the Internet in the State of Maryland implementation.
17	*"We first note that it is possible for an adversary to tamper with the voting terminals' ballot definition file (election.edb). If the voting terminals load the ballot definition from a floppy or removable storage card, then an adversary, such as a poll worker, could tamper with the contents of the floppy before inserting it into the voting terminal."*	M-7, M-89, O-7, O-14	LBEs do load ballots and a malicious worker could tamper with this process. Each LBE has policies and procedures in place, such as a two-person rule, to limit any single individuals access to voting terminals. The Logic and Accuracy testing preformed prior to the election, would uncover any falsified ballots.
17	*"On a potentially much larger scale, if the voting terminals download the ballot definition from the Internet, then an adversary could tamper with the ballot definition file en-route from the back-end server to the voting terminal. With respect to the latter, we point out that the adversary need not be an election insider; the adversary could, for example, be someone working at the local ISP."*	M-7, M-8, O-23	DRE devices are distributed with the approved ballots loaded and locked into the machine. The machines are sealed with tamper-proof tape prior to shipment to the polling site. The Election Judges remove the tamper-proof tape the morning of the election.
17	*"If a wireless network is used, anybody within radio range becomes a potential adversary. With high-gain antennas, the adversary can be sufficiently distant to have little risk of detection. If the adversary knows the structure of the ballot definition, then the adversary can intercept and modify the ballot definition while it is being transmitted. Even if the adversary does not know the precise structure of the ballot definition, many of the fields inside are easy to identify and change, including the candidates' names, which appear as plain ASCII text.10"*	O-23, O-24	Wireless networking is not used.
17	*"Let us now consider some example attacks that make use of modifying the ballot definition file. Because no cryptographic techniques are in place to guard the integrity of the ballot definition file, an attacker could add, remove, or change issues on the ballot, and thereby confuse the*	M-7, M-41, M-124, O-14, T-37	DRE devices are distributed with the approved ballots loaded and locked into the machine. The machines are sealed with tamper-proof tape prior to shipment to the polling site. The Election Judges remove the tamper-proof tape the morning of the election.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	result of the election."		tape the morning of the election.
17	*"Likewise, an attacker who can change the ballot definition could also change the ordering of the candidates running for a particular office. Since, at the end of the election, the results are uploaded to the server in the order that they appear in the ballot definition file, and since the server will believe that the results appear in their original order, this attack could also succeed in swapping the votes between parties in a predominantly partisan precinct. This ballot reordering attack is also discussed in more detail in Section 4.3."*	M-7, M-10	DRE devices are distributed with the approved ballots loaded and locked into the machine. The machines are sealed with tamper-proof tape prior to shipment to the polling site. The Election Judges remove the tamper-proof tape the morning of the election.
17	*"Suppose that the election officials are planning to download the configuration files over the Internet and that they are running late and do not have much time before the election starts to distribute ballot definitions manually (i.e., they might not have enough time to distribute physical media with the ballot definition files from central office to every voting precinct). In such a situation, an adversary could mount a traditional Internet denial-of-service attack against the election management's server and thereby prevent the voting terminals from acquiring their ballot definitions before the start of the election. To mount such an attack effectively, the adversary would ideally need to know the topology of the system's network, and the name of the server(s) supplying the ballot definition file.12 If a fair number of people from a certain demographic plan to vote early in the morning, then this could impact the results of the election."*	N/A	DRE devices are distributed with the approved ballots loaded and locked into the machine. The machines are sealed with tamper-proof tape prior to shipment to the polling site. The Election Judges remove the tamper-proof tape the morning of the election.
18	*"Unlike such traditional attacks, however, the network-based attack (1) is relatively easy for anyone with knowledge of the election system's network topology to accomplish; (2) this attack can be performed on a very large scale, as the central distribution point(s) for ballot definitions becomes an effective single point of failure; and*	O-23, O-24	The DRE devices are not connected to the Internet or to any other network. The DRE devices are distributed with the approved ballots loaded and locked into the machine. The machines are sealed with tamper-proof tape prior to shipment to the polling site. The Election Judges remove the tamper-proof tape the morning of the election.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	(3) the attacker can be physically located anywhere in the Internet-connected world, complicating efforts to apprehend the attacker. Such attacks could prevent or delay the start of an election at all voting locations in a state. We note that this attack is not restricted to the system we analyzed; it is applicable to any system that downloads its ballot definition files using the Internet."		tamper-proof tape the morning of the election.
18	*"Just as it is possible for an adversary to tamper with the downloading of the ballot definition file (Section 5.1), it is also possible for an adversary to tamper with the uploading of the election results. To make this task even easier for the adversary, we note that although the election results are stored "encrypted" on the voting devices (Section 4.4), the results are sent from the voting devices to the back-end server over an unauthenticated and unencrypted channel. In particular, CTransferResultsDlg::OnTransfer() writes ballot results to an instance of CDL2Archive, which then writes the votes in cleartext to a socket without any cryptographic checksum. Sending election results in this way over the Internet is a bad idea. Nothing prevents an attacker with access to the network traffic, such as workers at a local ISP, from modifying the data in transit."*	M-89, 0-23	The Internet is not used for transmitting voting counts.
18	*"If the voting terminals use a modem connection directly to the tabulating authority's network, rather than the Internet, then the risk of such an attack is less, although still not inconsequential. A sophisticated adversary (or employee of the local phone company) could tap the phone line and intercept the communication."*	O-23, O-24	Modem communications are subject to intercept. SAIC has recommended: a) encryption for the transmissions; b) a 100% verification of PCMCIA cards to the vote transmissions.
18	*"All of these adversaries could be easily defeated by properly using standard encryption suites like SSL/TLS, used throughout the World Wide Web for e-commerce security. We are puzzled why such a widely accepted and studied technology is not used by the voting terminals to*	O-23, O-24	Modem communications are subject to intercept. SAIC has recommended: a) encryption for the transmissions; b) a 100% verification of PCMCIA cards to transmissions.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	safely communicate across potentially hostile networks."		
18	*"In some configurations, where the voting terminals are directly connected to the Internet, it may be possible for an adversary to attack them directly, perhaps using an operating system exploit or buffer overflow attack of some kind. Ideally the voting devices and their associated firewalls would be configured to accept no incoming connections [CBR03]. This concern would apply to any voting terminal, from any vendor, with a direct Internet connection."*	O-23, O-24	The DRE device is not connected to the Internet or to any other network.
19	*"Of course, reading the source code to a product gives only an incomplete view into the actions and intentions of the developers who created that code. Regardless, we can see the overall software design, we can read the comments in the code, and thanks to the CVS repository, we can even look at earlier versions of the code and read the developers' commentary as they committed their changes to the archive."*	N/A	This is not a security requirement.
19	*"Inside cvs.tar we found multiple CVS archives. Two of the archives, AccuTouch and AVTSCE implement full voting terminals. The AccuTouch code dates to around 2000 and is copyrighted by "Global Election Systems, Inc." while the AVTSCE code dates to mid-2002 and is copyrighted by "Diebold Election Systems, Inc." (The CVS logs show that the copyright notice was updated on February 26, 2002.) Many files are nearly identical between the two systems and the overall design appears very similar. Indeed, Diebold acquired Global Election Systems in September, 2001.13 Some of the code, such as the functions to compute CRCs and DES, dates back to 1996, when Global Election Systems was called "I-Mark Systems."* *This legacy is apparent in the code itself as there are portions of the AVTSCE code, including entire classes,*	N/A	This is not a security requirement.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	that are either simply not used or removed through the use of #ifdef statements. Many of these functions are either incomplete or, worse, do not perform the function that they imply as is the case with *CompareFiles in Utilities/FileUtil.cpp:* *BOOL CompareFiles(const CString& file1, const CString& file2)* *{* */* XXX use a CRC or something similar */* *BOOL exists1, exists2;* *HANDLE hFind;* *WIN32_FIND_DATA fd1, fd2;* *exists1 = ((hFind = ::FindFirstFile(file1, &fd1)) != INVALID_HANDLE_VALUE);* *::FindClose(hFind);* *exists2 = ((hFind = ::FindFirstFile(file2, &fd2)) != INVALID_HANDLE_VALUE);* *::FindClose(hFind);* *return (exists1 && exists2 && fd1.nFileSizeLow == fd2.nFileSizeLow);* *}* *Currently the code will declare any two files to be the same*		

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	that have the same size. The author's comment to use a CRC doesn't make much sense, as a byte-by-byte comparison would be more efficient. If this code were ever used, its inaccuracies could lead to wide variety of subsequent errors. While most of the preprocessor directives that remove code correctly use #if 0 as their condition, some use #ifdef XXX. There is no reason that a later programmer should realize that defining XXX will cause blocks of code to be reincluded in the system (causing unpredictable results, at best). We also noticed #ifdef LOUISIANA in the code. Prudent software engineering would recommend a single implementation of the voting software, where individual states or municipalities could have their desired custom features expressed in configuration files."		
20	*"While the system is implemented in an unsafe language (C++), the code reflects an awareness of avoiding such common hazards as buffer overflows. Most string operations already use their safe equivalents, and there are comments reminding the developers to change others (e.g., should really use snprintf). While we are not prepared to claim that there are no buffer overflows in the current code, there are at the very least no glaringly obvious ones. Of course, a better solution would have been to write the entire system in a safe language, such as Java or C#."*	O-34	The scope of the risk assessment did not include a review of Diebold's software engineering practices. However, such an attack vector would require network access. The DRE devices are not connected to a network.
20	*"The core concepts of object oriented programming such as encapsulation are well represented, though in some places C++'s non-typesafe nature is exploited with casts that could conceivably fail. This could cause problems in the future as these locations are not well documented."*	N/A	This is not a security requirement.
20	*"Overall, the code is rather unevenly commented. While most files have a description of their overall function, the meanings of individual functions, their arguments, and the*	M-102	The scope of the risk assessment did not include a review of Diebold's software engineering practices. It should be noted that since the publication of the Rubin report, Diebold has

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	algorithms within are more often than not undocumented."		developed, documented, and implemented a change control process, which has been delivered to the SBE.
21	*"An important point to consider is how code is added to the system. From the CVS logs, we can see that most code updates are in response to specific bugs that needed to be fixed. There are numerous authors who have committed changes to the CVS tree, and the only evidence that we have found that the code undergoes any sort of review process comes from a single log comment: "Modify code to avoid multiple exit points to meet Wyle requirements." This could refer to Wyle Laboratories whose website claims that they provide all manner of testing services."*	M-3	The scope of the risk assessment did not include a review of Diebold's software engineering practices. It should be noted that since the publication of the Rubin report, Diebold has developed, documented, and implemented a change control process, which has been delivered to the SBE.
21	*"There are also pieces of the voting system that come from third parties. Most obviously is the operating system, either Windows 2000 or Windows CE. Both of these OSes have had numerous security vulnerabilities and their source code is not available for examination to help rule out the possibility of future attacks. Besides the operating system, an audio library called "fmod" is used.15 While the source to fmod is available with commercial licenses, unless the code is fully audited there is no proof that fmod itself does not contain a backdoor."*	M-3	Exploitation of these attack vectors would require network access. The DRE devices are not connected to a network.
21	*"Due to the lack of comments, the legacy nature of the code, and the use of third-party code and operating systems, we believe that any sort of comprehensive, top-to-bottom code review would be nearly impossible. Not only does this increase the chances that bugs exist in the code, but it also implies that any of the coders could insert a malicious backdoor into the system. The current design deficiencies provide enough other attack vectors that such*	M-3	The scope of the risk assessment did not include a review of Diebold's software engineering practices. However, such an attack vector requires network access. This risk is mitigated because the DRE devices are not connected to a network.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	an explicit backdoor is not required to successfully attack the system. Regardless, even if the design problems are eventually rectified, the problems with the coding process may well remain intact."		
21	*"While the code we studied implements a full system, the implementors have included extensive comments on the changes that would be necessary before the system should be considered complete. It is unclear whether the programmers actually intended to go back and remedy all of these issues as many of the comments existed, unchanged, for months, while other modifications took place around them. It is also unclear whether later version of AVTSCE were subsequently created."*	N/A	This is not a security requirement.
22	*"There are, however, no comments that would suggest that the design will radically change from a security perspective. None of the security issues that have been discussed in this paper are pointed out or marked for correction. In fact, the only evidence at all that a redesign might at one point have been considered comes from outside the code: the Crypto++ library16 is included in another CVS archive in cvs.tar. However, the library was added in September 2000 and was never used or updated. We infer that one of the developers may have thought that improving the cryptography would be useful, but then got distracted with other business."*	N/A	This is not a security requirement.

~~APPENDIX C:TABLE OF INTERVIEWS CONDUCTED DURING THIS REVIEW~~

~~In the course of our evaluation of the AccuVote-TS system, SAIC interviewed several people involved with the system with regards to the system, its setup, storage, operations and maintenance. Following is a list of the people interviewed for our review. These interviews were conducted between August 13, and August 18, 2003.~~

Date	Name	Title	Area
~~08/13/03~~	~~Susan Campbell~~	~~IT Specialist~~	~~Montgomery County~~
	~~Paul Valette~~	~~Manager, Election Operations~~	
~~08/13/03~~	~~Robin Downs~~	~~Elections Administrator~~	~~Prince George's County~~
	~~Hugh Alexander~~	~~IT Consultant~~	
	~~Alicia Alexander~~	~~Assistant to the Administrator~~	
~~08/14/03~~	~~Julie Och~~	~~Chief Judge~~	~~Montgomery County~~
	~~Paul Valette~~	~~Manager, Election Operations~~	
	~~Charles Deegan~~	~~President BOE~~	~~Prince George's County~~
	~~Carl Ruble~~	~~Vice President BOE~~	
	~~John P. Morrissey~~	~~Attorney~~	
	~~Daniel Lee~~	~~Chief Judge~~	
	~~Harold Rustin~~	~~Manager, Election Operations~~	
~~08/15/03~~	~~David Heller~~	~~Project Manager~~	~~SBE~~
	~~Tom Feehan~~	~~Diebold Engineer~~	~~Diebold~~

~~Date~~	~~Name~~	~~Title~~	~~Area~~
~~08/18/03~~	~~Donna Duncan~~	~~Director~~	~~SBE~~
	~~Pam Woodside~~	~~CIO~~	~~SBE~~

~~APPENDIX D:~~APPENDIX C: TABLE OF DOCUMENTS REVIEWED DURING THIS ASSESSMENT

In the course of our evaluation of the AccuVote-TS system, SAIC reviewed all available documentation pertaining to the system, its setup, storage, operations and maintenance. Following is a list of the documents considered in our review. The document review commenced on August 5, and was completed August 20, 2003.

File Name if Electronic	Actual Title
2002 AG Instructions DRE	INSTRUCTIONS OF THE ATTORNEY GENERAL OF MARYLAND TO THE REGISTERED VOTERS OF MARYLAND FOR THE OPERATION OF ACCUVOTE – TS VOTING UNITS
2002 AG Instructions Writein	INSTRUCTIONS FOR WRITE-IN VOTES
2002 Allegany County Manual	ELECTION JUDGES TRAINING AND PROCEDURES
2002 general probs (must be AG)	N/A
4-30-03i	DRE Open Issues
05-14-03i	DRE Open Issues
05-21-03i	DRE Open Issues
05-07-03i	DRE Open Issues
09-15-02p	RECOMMENDATIONS GUBERNATORIAL PRIMARY ELECTION 2002

File Name if Electronic	Actual Title
	MONTGOMERY COUNTY
AGTouchScreen	INSTRUCTIONS OF THE ATTORNEY GENERAL OF MARYLAND TO THE REGISTERED VOTERS OF MARYLAND FOR THE OPERATION OF ACCUVOTE – TS VOTING UNITS
AGWrite-In	INSTRUCTIONS FOR WRITE-IN VOTES
AlleganyGeneralFlowChart	Ballot Creation Process for Allegany County
Codeof Conduct	CODE OF CONDUCT FOR VOTER EDUCATION FACILITATORS
CommPlan	SBE Communications Plan
ContractMod	INFORMATION TECHNOLOGY CONTRACT MODIFICATIONS SBE Voting System Implementation Project State Board of Elections (SBE) PROGRAM
DorchesterGener…	Ballot Creation Process for Dorchester County
DRIMPlan	SBE Disaster Recovery and Incident Management Plan
DRIMTemplate	Disaster Recovery and Incident Management Plan
Export	General Election Results Export Procedure
FinalChangeControl	SBE Change Control Plan
FinalMaintenancePlan	SBE Maintenance Plan
How to Configure a TS to Transfer Results	How to Configure a TS to Transfer Result

File Name if Electronic	Actual Title
ImplementationPlan	SBE Implementation Plan
Judge's TS What If's	AccuVote TS - Technician's What If's
L&Acertificate1	CERTIFICATION # 1 (Inspector) ACCUVOTE TS PRE-ELECTION LOGIC AND ACCURACY TESTING
L&Acertificate2	CERTIFICATION # 2 (Inspector) ACCUVOTE TS PRE-ELECTION LOGIC AND ACCURACY TESTING
L&Acertificate3	CERTIFICATION # 3 (Inspector) ACCUVOTE TS PRE-ELECTION LOGIC AND ACCURACY TESTING
L&Acertificate4	CERTIFICATION # 4 (Inspector) ACCUVOTE TS PRE-ELECTION LOGIC AND ACCURACY TESTING
L&Acertificate5	CERTIFICATION # 5 (Inspector) ACCUVOTE TS PRE-ELECTION LOGIC AND ACCURACY TESTING
L&AChecklist	AccuVote-TS L&A Checklist
L&ADeclaration	BOARD OF ELECTIONS COMPUTER PROFESSIONAL DECLARATION AND CONFIDENTIALITY AGREEMENT
MontgomerGeneralFlowChart	Ballot Creation Process for Montgomery County
PCMCIA.Recovery	Election Recovery PCMCIA Failure Election in Progress
Performing the LA pre-election setup checks	L&A Testing Revised 10/09/02
PhaseII_IP	State Board of Elections, AccuVote Touch Screen Voting System Phase II Implementation Plan June 19, 2003
PollworkerManual	WELCOME TO DIEBOLD POLL WORKER TRAINING

File Name if Electronic	Actual Title
PowerManagementPlan	State Board of Elections, AccuVote Voting System Power Management Plan
PrinceGeorgeGeneralFlowChart	Ballot Creation Process for Prince George's County
QAPlan	State Board of Elections Systems Project Management Office Support Quality Assurance (QA) Plan
RISCPlan	State Board of Elections Systems Project Management Office Support Risks, Issues, Systems Incidents, and Changes (RISC) Plan
Software_Hrdwr Changes	Software/Hardware Changes to Diebold Elections Systems
SpaceRequirements4-03	PHASE II IMPLEMENTATION SPACE AND ELECTRICAL REQUIREMENTS BY COUNTY
TECHNICIANS Election Day Check Lists	TECHNICIANS' MORNING CHECK LIST
Tech's TS What If's	AccuVote TS - Technician's What If's
TS UNIT DEFECT BREAKDOWN	TS UNIT DEFECT BREAKDOWN
TSAccumulate	Using the AccuVote TS
TSAccumulateNoWrite	Using the AccuVote TS
TSClose	Using the AccuVote TS
TSModem	Using the AccuVote TS
TSOpen	Using the AccuVote TS
TSVIBS	Using the AccuVote TS
VCProgrammer 4.1 User's Guide Revision 3.0	VC Programmer Guide 4.1

File Name if Electronic	Actual Title
Voter Card Encoder User's Guide Revision 1.3	Voter Card Encoder User Guide
VoterAccessCard	Front side of card
WarehouseStandard4-03	Diebold Warehouse Standards
WBSPlan	WBS Plan
20981KeyboardAttachment-20040211	Santa Clara RFP
checksandbalances	July 30, 2003 Diebold - Checks and balances in elections equipment and procedures prevent alleged fraud scenarios
diebold JHU Study	Analysis of an Electronic Voting System Aviel. D. Rubin, et al, July 23, 2003
georgia	Security in the Georgia Voting System Britain J. Williams, Ph.D. April 23, 2003
	Board of Election – PG County 2002 Voting Machine Technician's Guide
	Board of Election – PG County 2002 Quick Reference Guide
	Procedures for Official Canvass, Verification and Post-Election Audit
	Allegany County – AccuVote Manual
	SBE Procedures for Election Day
	Diebold – AccuVote-TS R6 1.2

File Name if Electronic	Actual Title
	Diebold – Election Administrator's Guide
	Diebold – Ballot Station 4.3 User's Guide
	Diebold – Voting System – Phase II Election Judge Manual
	Precinct Count 1.96 User's Guide , Revision 2.0, Diebold Election Systems
	Wyle Test Report, Change Release Report of the Accuvote-TS R6 DRE Voting Machine (Firmware Change Release 4.3.15)
	Diebold Election Systems Software Qualification test Report GEMS 1-18, Addendum 2, 7/08/03, Ciber, Inc.
	Memo from Lamone – 2002 Election Results Transfer
	State-Wide Voting System Project Election Night Report Procedures
	SBE Recount Process Workflow for the AccuVote Voting System
	Auditability of Non-Ballot, Poll-Site Voting Systems
	Part II. Position Functions
	Procedures for Official Canvass Verification and Post-Election Audit
	Memorandum Election Day Log
	Registration & Election Laws of MD
	DRE Voting System Contact
	MD Certification Evaluation of the Global Election Systems, Inc AccuTS R6
	Diebold – Poll Worker Training

File Name if Electronic	Actual Title
	SBE Work Breakdown Structure
	SBE Communication Plan
	SBE Risks, Issues, System Incidents & Changes
	Registration and Election Laws of Maryland
	Diebold Pollworker's Guide
	Election Judges Training & Procedures
	Diebold AccuVote-TS R6 Hardware Guide
	Diebold – User's Guide
	SBE – Phase II Implementation Plan
	Information Technology Contract Modifications
	Recommendations Gubernatorial Primary Election 2002
	Memorandum Emergency Contingency Plan
	Gubernatorial General Election Night Results Processing, September 10, 2002
	Gubernatorial General Election Night Results Processing, November 5, 2002
	2002 Gubernatorial Primary Election Results Tracking Worksheet
	2002 Gubernatorial General Election Results Tracking Worksheet
	2002 Gubernatorial General Election SBE Staffing Worksheet
	State-Wide Voting System Project General Election Results Export Procedures

File Name if Electronic	Actual Title
	Board of Election – PG County 2002 Election Judge Manual
	Prince George's County Government, Office of Information Technology and Communications, Letter to Linda Lamone, Administrator, Regarding Concerns and Recommendation on Accuvote –TS systems.
	Diebold Poll Worker Training Guide
	SBE AccuVote-TS Direct Recording Electronic Voting System Certification
	State-Wide Voting System Project, Touchscreen and Booth Acceptance Test Guide
	State-Wide Voting System Project, UPS Acceptance Test Guide
	State-Wide Voting System Project, OS Acceptance Test Guide
Diebold Source Code, version 4.3.1.5	Diebold Source Code, version 4.3.1.5, received 15 August 2003
CD	PG County – Taking Charge Election Judge Training
CD	Montgomery County – Training Materials Election Judge & Tech. Staff
CD	Montgomery Judge's Manual Complete
Video	"From Chads to Bytes"

Documentation Received After – Wed-08/14

File Name if Electronic	Actual Title

File Name if Electronic	Actual Title
GA – Certification Test Report 2003	Certification Test of GA
GA – LCCR Analysis – Voter Verification	*ELECTION REFORM POLICY ANALYSIS:* "Voter-Verified Paper Trails" Are Not Needed To Keep Elections From Being Stolen
GA – Security – 08	Security Features of Georgia's Electronic Voting System
GA – Voting system security	Security in the Georgia Voting System (duplicate)