Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
O-94	Voters must be authenticated to the system, using established procedures.	M	Election Judges' Manual establishes procedures to authenticate voters to the DRE as directed in Election Law Article, § 10-310		
O-95	A post election audit must be conducted in order to reconcile and ensure that the number of voters equals the number of votes, and the votes were accurately collected.	M	Procedures for Official Canvass, Verification and Post-Election Audit are conducted in order to reconcile and ensure that the number of voters equals the number of votes, and the votes were accurately collected. Note: Only 10% validation is currently performed and actual transmissions become official record after canvassing. We recommend the canvassing of 100% of the precincts once the DRE is deployed statewide. The time to perform a 100% is minimal and would validate pre-election testing.		
O-96	SBE will ensure that, local LBE election boards conduct and document Logic and Accuracy Tests of every DRE voting terminal prior to election day.	M	Each LBE conducts Logic and Accuracy Test and Certification on each DRE voting terminal.		
O-97	SBE will ensure that, local election boards conduct and document a system verification test on every voting unit within.	M	Each LBE conducts Logic and Accuracy Test and Certification on each DRE voting terminal.		
O-98	SBE will ensure that the system shall permit voting in secrecy.	M	The Election Judge and Polling officials follow procedures in the Election Judge's Manual to protect secrecy in the voting process. The DRE voting terminals block		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	taking the signed VAC to the next step in the voting process.		and instruct the voter on taking the signed VAC to the next step in the voting process. These VAC cards are used to verify the vote totals at the conclusion of the election against the vote totals stored in the DRE memory. Also if a DRE were damaged or destroyed during an election such that the vote data for votes already cast could not be retrieved from the machine, the State of Maryland could use the VACs for that machine to contact the affected voters to have them return to the polling station and recast their votes. The next step in the voting process is for the voter to present his or her VAC to the election official responsible for the DRE terminal. The election official takes the voter's VAC and activates a DRE Voter Access Card smartcard for that voter. The election official places the VAC in the envelop associated with the DRE terminal and permits the voter to insert the DRE Voter Access Card smartcard into the DRE to vote.		
O-104	Local election boards will ensure that the judges manual provides detailed poll closing procedures including: a) How to document public and protective counter totals; b) How to end the election; c) How to print and sign the vote total reports; d) How to post the vote totals reports; e) How to remove the memory cards from the voting	M	The judges manual provides detailed poll closing procedures including: a) How to document public and protective counter totals; b) How to end the election; c) How to print and sign the vote total reports; d) How to post the vote totals reports; e) How to remove the memory cards from the voting units; f) How to return the materials to the local board office.		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~units; f) How to return the materials to the local board office.~~				
~~O-105~~	~~If a consolidation of memory cards is used, the Election Judges shall perform the consolidation in accordance with the election judges manual.~~	~~M~~	~~According to interviews with Election Judges, they perform the consolidation and verification of the vote totals in accordance with the Election Judge Manual.~~		
~~O-106~~	~~Local boards shall develop and SBE shall approve procedures for returning priority items to the local board after closing the election.~~	~~M~~	~~Each LBE has procedures for returning priority items to the local board after closing the election in the Election Judge Manual to prevent high priority items from being lost or stolen.~~		
~~O-107~~	~~Local boards shall develop and SBE shall approve procedures for aggregating precinct counts which will include written procedures for: a) Assembling memory cards from each polling place; b) Transferring votes from the memory cards to the EMS; c) Manually entering absentee ballot results into the EMS; d) Aggregating vote counts for the entire county; e) Securing the physical area where the tabulation takes place; f) Controlling access to the area, including documentation for who may be admitted to the area, by name or job function.~~	~~M~~	~~Each LBE Election Judge Manual has procedures approved by the SBE to: a) Assembling memory cards from each polling place; b) Transferring votes from the memory cards to the EMS; c) Manually entering absentee ballot results into the EMS; d) Aggregating vote counts for the entire county; e) Securing the physical area where the tabulation takes place; f) Controlling access to the area, including documentation for who may be admitted to the area, by name or job function.~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
~~O-108~~	~~Local boards shall develop and SBE shall approve procedures for tabulation of write-in votes which: a) In a general election, the results report produced by the voting unit shall indicate the number of votes cast in each write-in position for each contest; b) The results memory card shall contain the names of individuals for whom voters cast write-in votes and shall copy those names to the EMS; c) Require the production of a printed report of all write-in votes, which shall be tallied, recorded, and reported.~~	~~M~~	~~The Ballot Creation Process establishes the ballot to include write-in votes. The Logic and Accuracy Test and Checklist is used to verify the tabulation of the write-in votes prior to each election.~~		
~~O-109~~	~~On completion of pre-election testing, the local board shall secure master copies of the ballot control logic in a secure, locked location, designated by the local board, but separate from the location of the working copies. They shall be retained as required by law, court order, or SBE directive.~~	~~M~~	~~The LBE securely stores a master copy of the ballot separate from the location of the working copies.~~		
~~O-110~~	~~The local board shall develop a plan for retaining and storing memory cards, consolidation reports and other data processing materials related to the election. The plan shall be consistent with the Election~~	~~M~~	~~Each LBE retains and stores memory cards, consolidation reports and other data processing materials related to the election, consistent with the Election Records Management Program and approved by the State Administrator. Storage of this information is in a secure~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~Records Management Program and be approved by the State Administrator. Storage shall be in a locked location and for such time until the period for challenging the election expires and for any additional time required by law or Regulation.~~		~~location and is retained for such time until the period for challenging the election expires and for any additional time required by law or Regulation.~~		

Technical Controls

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
T-1	To ensure vote accuracy, SBE will ensure that all systems include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy.	U	If SBE does not ensure that all systems include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy, then the data could be modified or deleted when transmitted and system integrity would be compromised. The PCMCIA flash memory card used to store the election results does not contain any cryptographic hashes that could be used to verify the data integrity before and after transmission and verification. **Likelihood: LOW** Based on the existing security control of manual data reconciliation, there is little danger of data corruption becoming a critical issue. **Impact: MEDIUM** If data is modified or deleted during submission, there is no automated parity checking, and it becomes necessary to use manual reconciliation, then the time allowed for vote tallying could greatly increase.	**LOW**	Perform automated cryptographic hash creation once data is entered, then check that hash once the data has been transmitted to the destination.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
~~T-2~~	~~To ensure vote accuracy, SBE will ensure that all systems provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected.~~	~~M~~	~~All of the system functions are logged whenever an action occurs during setup as well as during normal operation.~~		
~~T-3~~	~~SBE will ensure that a consolidated printed report of the results for each contest of all votes cast that includes the votes cast for each selection, the count of undervotes, and the count of overvotes is produced.~~	~~M~~	~~The DRE voting machines print out a report of the results of each station during the post-election using the internal printing device. This report includes the votes cast for each selection, the count of undervotes, and the count of overvotes.~~		
~~T-4~~	~~SBE will ensure controls are implemented to ensure that there is no access path from unofficial electronic report or files to the storage devices for official data.~~	~~M~~	~~SBE has documented procedures that require the transfer of data from the DRE voting machine to the GEMS server only occur while the DREs are in the same physical location, or utilize point-to-point communications.~~		
~~T-5~~	~~SBE will ensure controls are implemented to clearly indicate on each unofficial report or file that the results it contains are unofficial.~~	~~M~~	~~SBE has processes in place to ensure controls are implemented to clearly indicate on each unofficial report or file that the results it contains are unofficial.~~		
~~T-6~~	~~SBE will ensure security controls are implemented to identify fraudulent or erroneous changes to the system.~~	~~U~~	~~If SBE does not ensure security controls are implemented to identify fraudulent or erroneous changes to the system, then it is very difficult to identify when any improper use of the system has occurred~~	~~HIGH~~	~~Windows 2000 OS on the GEMS server should be configured to audit all security events that are generated. These logs should be reviewed on a regular basis, archived for future use, and protected~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			improper use of the system has occurred and system integrity may be compromised. **Likelihood: HIGH** Audit logs on the GEMS server are not configured to log any security events, or any extended system information. **Impact: HIGH** Both intentional and unintentional human threats can cause damage to the system, and no audit records are stored to determine if damage occurred.		archived for future use, and protected from unauthorized disclosure. Additionally, administrative user accounts should not be shared by multiple users.
T-7	SBE will ensure security controls are implemented to prevent alteration of voting system audit trails.	M	The voting system software only allows users with a Supervisor card to purge log entries and backup data.		
T-8	SBE will ensure security controls are implemented to prevent introduction of data for a vote not cast by a voter.	M	If SBE does not ensure security controls are implemented to prevent introduction of data for a vote not cast by a voter, then the vote data would be inaccurate and system integrity would be compromised. Only voters with a valid Voter Access Card can cast votes.		
T-9	SBE will ensure security controls are implemented that require all systems that transmit data over public	U	If SBE does not ensure security controls are implemented that require all systems that transmit data over public telecommunications networks to employ	**HIGH**	The DRE voting terminal should contain a cryptographic signature that is unique to each terminal. Cryptographic signatures, those based on a session identifier, rather

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~telecommunications networks to employ digital signature for all communications between the vote server and other devices that communicate with the server over the network.~~		~~digital signature for all communications between the vote server and other devices that communicate with the server over the network, then the data sent from a DRE voting terminal cannot be positively identified as valid data and system integrity may be compromised.~~ ~~Digital signatures are not used to protect and verify the integrity of the election data while it is in transit over the public switched telephone network.~~ ~~**Likelihood: HIGH**~~ ~~In order to exploit this vulnerability, a malicious threat source would need to have knowledge of the particular telecommunications network on which this data would be traveling and the ability to intercept the traffic without either end noticing interception.~~ ~~**Impact: HIGH**~~ ~~If a malicious threat source were able to compromise the data in transit, then they would be able to substitute invalid data for valid data, causing inaccurate results for the election.~~		~~than a static ID, are difficult to forge and should be used.~~
~~T-10~~	~~SBE will ensure security controls are implemented that require all systems that transmit data over public telecommunications networks to require that at least two~~	~~M~~	~~In order to process ballots, both the DRE voting terminal and the GEMS server must be in the mode to do so, which requires a Supervisor Access Card for the terminal, and administrator login rights for the GEMS software. These~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~authorized election officials activate any critical operation regarding the processing of ballots.~~		~~rights are only given to authorized election officials, each of whom adheres to the two officials rule.~~		
~~T-11~~	~~SBE will implement security controls to create and preserve an audit trail of every vote cast during the period of interrupted communication and system operation.~~	~~M~~	~~All of the voting terminals have an internal battery that powers the system in the event of power loss, and there is an Uninterruptible Power Supply (UPS) for the GEMS server that tallies votes, as well. If the DRE voting terminal had communication problems, the data is stored on a non-volatile flash memory card. Even once the card is reset for a new election, a backup file is kept on the card unless purged by a Supervisor Access Card. Any ballot that was created but does not have any results transmitted after an election close will be flagged by the GEMS software.~~		
~~T-12~~	~~Anti-virus tools should be used to detect, identify, or remove viruses.~~	~~U~~	~~If anti-virus tools are not used to detect, identify, or remove viruses, then there could be serious threats to the availability of the voting service.~~ ~~There is no anti-virus software installed on the GMES voting server.~~ ~~**Likelihood: MEDIUM**~~ ~~Although neither the DRE voting terminal nor the LBE GEMS servers will be connected to any publicly available network, it is possible that during system updates, viruses could be introduced to~~	~~**MEDIUM**~~	~~Ensure that anti-virus software is used on the GEMS voting server, and that anti-virus definition files are updated regularly.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			the system. **Impact: HIGH** A virus could cause problems as severe as data corruption and data deletion on both the DRE voting terminals and the GEMS servers.		
T-13	Systems should implement DAC or MAC.	M	Both the GEMS server and the DRE voting terminals practice discretionary and mandatory access controls over the data.		
T-14	Cryptographic keys must be securely managed when cryptographic functions are implemented in various other controls. (Cryptographic key management includes key generation, distribution, storage, and maintenance).	N/A	Cryptographic keys are not used in the AccuVote-TS voting machines.		
T-15	Organization IT systems and networks that employ routable protocol devices shall contain intrusion detection systems (IDS).	P	If IDS systems are not installed to detect network intrusions and potential breaches in progress, then unauthorized access may be undetected and information may be modified and deleted resulting in the potential loss of confidentiality, integrity, and availability of system data. The LBE GEMS voting server and the DRE voting are not connected to a publicly available network that might contain an external interface that would	**HIGH**	Remove the SBE GEMS server from network and rebuild entire system from trusted media to assure and validate system has not been compromised. Do not put any software other than the GEMS software on the system. Locate the server in a secure location.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			necessitate the use of IDS. The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. **Likelihood: HIGH** SBE currently has a GEMS server used to generate and distribute ballots with no security mechanisms in place. The ballots are distributed to the LBEs for proofing and Logic and Accuracy Testing before the election; however the Logic and Accuracy Testing does not role the date ahead to check for Trojan software. **Impact: HIGH** An attacker could use this server to change the initial ballot and possibly place a Trojan software within the ballot data.		
T-16	IDS systems shall be installed with boundary protection devices (e.g., firewalls) and/or routers to detect network intrusions and potential breaches in progress at all points external to the SBE network and when the risk analyses dictate an IDS on internal networks.	N/A	The LBE GEMS voting server and the DRE voting are not connected to a publicly available network that might contain an external interface that would necessitate the use of IDS. The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15.		
T-17	IDS systems shall be installed on voting system collection	N/A	The LBE GEMS voting server and the DRE voting are not connected to a		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	server to detect intrusions.		publicly available network that might contain an external interface that would necessitate the use of IDS. The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15.		
T-18	SBE networks shall be protected by boundary protection devices (firewalls and trusted guards) at identified points of interface with lesser or unsecured networks. These security devices and configurations shall be designed and implemented employing a system security engineering/risk management process.	N/A	The LBE GEMS voting server and the DRE voting are not connected to a publicly available network that might contain an external interface that would necessitate the use of firewalls. The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15.		
T-19	Firewalls shall define and implement a network security policy based on an engineering/risk management process.	N/A	The LBE GEMS voting server and the DRE voting are not connected to a publicly available network that might contain an external interface that would necessitate the use of firewalls. The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15.		
T-20	Firewalls shall block all services not required and disable unused ports.	N/A	The LBE GEMS voting server and the DRE voting are not connected to a publicly available network that might contain an external interface that would		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			necessitate the use of firewalls. The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15.		
T-21	Firewalls shall hide and prevent direct accessing of Department trusted network addresses from untrusted networks.	N/A	The LBE GEMS voting server and the DRE voting are not connected to a publicly available network that might contain an external interface that would necessitate the use of firewalls. The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15.		
T-22	Firewalls shall maintain comprehensive audit trails.	N/A	The LBE GEMS voting server and the DRE voting are not connected to a publicly available network that might contain an external interface that would necessitate the use of firewalls. The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15.		
T-23	Firewalls shall fail in a closed state.	N/A	The LBE GEMS voting server and the DRE voting are not connected to a publicly available network that might contain an external interface that would necessitate the use of firewalls. The SBE GEMS server is connected to the SBE Intranet, which has access to		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			~~the Internet. This risk is analyzed in requirement T-15.~~		
~~T-24~~	~~Firewalls shall operate on a dedicated platform (device).~~	~~N/A~~	~~The LBE GEMS voting server and the DRE voting are not connected to a publicly available network that might contain an external interface that would necessitate the use of firewalls.~~ ~~The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15.~~		
~~T-25~~	~~Downloading of mobile code and executable content from a controlled interface between interconnected systems shall be permitted only when a boundary protection device appropriately configured (to handle such a download) is in place and approved by the SBE.~~	~~N/A~~	~~The LBE GEMS voting server and the DRE voting are not connected to a publicly available network.~~ ~~The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15.~~		
~~T-26~~	~~Operating systems should be configured to set ACLs/Permissions for system files, administrative tools, system registry entries, and files that control security services in applications.~~	~~M~~	~~The voting server has the appropriate ACLs/Permissions for system files for the system files, administrative tools, system registry entries, and files that control security services in applications.~~		
~~T-27~~	~~Operating systems should be configured to enforce password history to 24 passwords remembered.~~	~~U~~	~~If operating systems are not configured to enforce password history to 24 passwords remembered, then users could recycle commonly used~~	~~**MEDIUM**~~	~~Configure the GEMS voting server to enforce password history to 24.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	remembered.		passwords, thereby reducing the effective security of those passwords and system integrity may be compromised. The GEMS voting server does not enforce password history. **Likelihood: MEDIUM** Access to the GEMS server is limited. **Impact: HIGH** This vulnerability could be exploited by a malicious insider gaining knowledge of a valid user's password that was required to be changed, but was then changed back to the original password. This could allow unauthorized users access to the sensitive voting data.		
T-28	Operating systems should be configured to set minimum password age to 1 day and maximum password age to 90 days.	U	If operating systems are not configured to set minimum password age to 1 day and maximum password age to 90 days, then password controls may be ineffective and it may be possible for unauthorized users to gain access to privileged data and system integrity may be compromised. Operating systems are not configured to set minimum password age to 1 day and maximum password age to 90 days. Passwords should not be changed too rapidly, or some users will set a newly changed password to one they have used previously. The longer a password	**MEDIUM**	Configure the GEMS voting server to enforce a minimum password age of 1 day and a maximum password age of 90 days.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			is used the more likely it is that the password will be intercepted by a malicious user. The GEMS voting server does not enforce minimum or maximum password age. **Likelihood: HIGH** Effective password controls are not currently in place. **Impact: HIGH** If a malicious insider were to intercept or acquire a valid user's password, they could gain access to privileged data.		
T-29	Only administrators should have the ability to add, change, or remove system or application level files.	M	The users profile for the GEMS voting server have the appropriate access controls set for the system files, administrative tools, system registry entries, and files that control security services in applications.		
T-30	Operating systems should be configured to lock the desktop of the current user after fifteen minutes of inactivity and to lock out the account of any user that has three invalid login attempts.	U	If operating systems are not configured to lock the desktop of the current user after fifteen minutes of inactivity and to lock out the account of any user that has three invalid login attempts, then it is possible for the user to walk away and leave the server open for some other person to use. Not having an account become locked after 3 tries makes it much easier for passwords to be guessed. System confidentiality,	**HIGH**	Set the default screensaver timeout to 15 minutes and to require a password to unlock. Set the account lockout policy to deny access after 3 failed attempts.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			integrity, and availability may be compromised. The GEMS voting server does not have a desktop timeout set, nor does it lock an account after 3 failed login attempts. **Likelihood: HIGH** The controls are not effective to prevent a motivated threat source from exploiting this vulnerability. The lack of a session timeout and unlimited login attempts, coupled with the fact that the auditing control is not effectively utilized result in a high likelihood that this vulnerability would be exploited. **Impact: HIGH** If a malicious user were to access a computer that was left unlocked by a valid user, then they would have access to the same resources and data that user normally has. Without an account lockout count, then a malicious user can use a brute-force attack to guess a user's password, again gaining access to the valid user's resources and data.		
T-31	In low-risk environments, the event logs should be used weekly to review the log files; in higher risk environments, log files should be reviewed daily when in operation.	U	If event logs are not regularly reviewed, then it is very difficult to identify when any improper use of the system has occurred and system confidentiality and integrity may be compromised. Event logs on the server are not	HIGH	Event logs should be reviewed on a regular basis.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			reviewed on a regular basis. **Likelihood: HIGH** Without event log review, inappropriate activity may not be detected. **Impact: HIGH** Both intentional and unintentional human threats can cause damage to the system and without audit log review, inappropriate system activity may not be detected. Exercise of this vulnerability could result in significant impairment to the SBE mission.		
T-32	The "Require logon to change the password" parameter is required so that users are logged on a system before they can change their password. If a password has expired and the users are currently not logged on a system, a System Administrator (SA) must log on to change the user password.	M	Users must logon to the system to change their password or have the System Administrator change their password if they are not logged on and their password is expired.		
T-33	Passwords should meet State of Maryland Security Standards.	U	If passwords do not meet State of Maryland Security Standards, then easily guessable passwords may allow unauthorized access to the system resulting in the potential loss of confidentiality, integrity, and availability. Passwords are not required to have any	**HIGH**	Create a local security policy that enforces the password security policies of the State of Maryland. Ensure that the passwords are properly configured on all voting system components.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			password complexity or minimum length. **Likelihood: HIGH** Effective password controls are not currently in place. **Impact: HIGH** A malicious user could guess passwords and possibly gain the ability to take over and replace processes, and access other computers on the network.		
T-34	System should be configured to prompt user to change password 14 days before its expiration.	N/A	Passwords are not currently set to expire.		
T-35	Maximum log size should be set to record all necessary events or comply with local logging policy and installed hardware limitations.	U	If the maximum log size is not set to record all necessary events or comply with local logging policy and installed hardware limitations, then it is possible that events that were not reviewed would be deleted in order to reuse space and audit trails would be lost. The maximum log size for Windows 2000 GEMS server was set to 512 kilobytes and events to be overwritten after 7 days. This is insufficient to trace events that could cause problems with the voting system. **Likelihood: HIGH** This control is not effective for retaining	**HIGH**	Set the maximum log to an appropriate size.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			system and security events pertinent to the voting system. **Impact: HIGH** Without a large enough maximum log size, an attacker or malicious user could generate a large number of system events, causing log entries to be overwritten. Exercise of this vulnerability could result in significant impairment to the SBE mission.		
T-36	Appropriate encryption software should be used for protecting sensitive information on a mobile computer/laptop.	N/A	No mobile computers or laptops are used as part of the voting system.		
T-37	Use of encryption is required when sensitive information is transmitted over an un-trusted public network domain (e.g., the Internet).	N/A	The LBE GEMS voting server and the DRE voting are not connected to a publicly available network. The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15. It should be noted, that FTP is used; see O-14; modem transmissions are used; see T-42 below.		
T-38	System accounts will not be shared.	U	If system accounts are shared, it is not possible to trace events to individuals and system confidentiality, integrity, and availability may be compromised.	**HIGH**	Require that all system users have their own accounts.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~System accounts are shared.~~ ~~**Likelihood: HIGH**~~ ~~Systems accounts are shared. There are no other accounts on the machine beside the administrator, AccuVote, and accutouch accounts. Each user that is authorized for the machine should have their own account to ensure accountability.~~ ~~**Impact: HIGH**~~ ~~If a malicious user gains access to a shared system account, it would be very difficult to trace the actions of a legitimate system user versus those of the malicious user. Exercise of this vulnerability could result in significant impairment to the SBE mission.~~		
~~T-39~~	~~All system access by privileged users will be logged by the system.~~	~~U~~	~~If all system access by privileged users is not logged by the system, then it is not possible to trace events to individuals and system confidentiality, integrity, and availability may be compromised.~~ ~~Audit logs on the server are not configured to log security events.~~ ~~**Likelihood: HIGH**~~ ~~Without auditing privileged user access, inappropriate activity may not be detected.~~	~~**HIGH**~~	~~Windows 2000 Server should be configured to audit all security events that are generated.~~

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~Impact: HIGH~~ ~~Both intentional and unintentional human threats can cause damage to the system and without audit log review, inappropriate system activity may not be detected. Exercise of this vulnerability could result in significant impairment to the SBE mission.threats can cause damage to the system, and no audit records are stored to determine if damage occurred.~~		
~~T-40~~	~~The system bootstrap, monitor, and device controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote-counting program, and its associated exception handlers.~~	~~M~~	~~The firmware cannot be updated by any process from the voting server or the voting terminal itself.~~		
~~T-41~~	~~The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as computer chip) other than the component on which the operating system resides.~~	~~M~~	~~On the voting terminals, the operating system is located internally, while the election information is located both internally and on a removable PCMCIA flash memory card.~~		
~~T-42~~	~~Cryptography should be considered for data that is~~	~~U~~	~~If cryptography is not used for data that is sensitive, has a high value, or~~	~~HIGH~~	~~Implement cryptographic protocols for the data while it is transit such as hardware~~

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~sensitive, has a high value, or represents a high value if it is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage.~~		~~represents a high value if it is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage, then data in transit and data at rest may be subject to unauthorized access and the confidentiality, integrity, and availability of the data may be compromised.~~ ~~Although the data is transmitted over a private point-to-point network, no cryptography is used to ensure the integrity of the data being passed.~~ ~~**Likelihood: HIGH**~~ ~~A motivated threat source could intercept the unencrypted data in transit. Access to communications closets at polling places, such as public schools, is not likely to be highly secured.~~ ~~**Impact: HIGH**~~ ~~A malicious user could intercept the data and modify it or copy it during transmission.~~		~~link-layer encryption (encrypting modems using 3DES or better encryption) or application-layer encryption (Secure Sockets Layer [SSL], Transport Layer Security [TLS], etc.).~~
~~T-43~~	~~Individual ballot images in memory must be randomized to protect voter secrecy.~~	~~U~~	~~If individual ballot images in memory are not randomized to protect voter secrecy, then it is possible to tie votes back to specific individuals and system confidentiality may be compromised.~~ ~~Individual ballots are stored sequentially.~~	~~**LOW**~~	~~Implement a function to randomize the write location of the individual ballot images.~~

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~**Likelihood: LOW**~~ ~~The likelihood is remote that individual vote records could be reconstructed due to the amount of collusion required to exploit this vulnerability.~~ ~~**Impact: LOW**~~ ~~The impact is low because it would affect a limited number of voters.~~		
~~T-44~~	~~SBE will ensure that voting units be maintained such that the voting mechanism can not be reopened to voting after: a) The manager card is inserted in to the card reader; b) The election judge's PIN number is entered on the screen; c) The "End Election" button is pressed.~~	~~M~~	~~SBE has processes in place to prevent the voting terminal from being reopened once the close of voting has taken place.~~		
~~T-45~~	~~SBE will ensure that the Election Management System shall tabulate and report the total votes cast for each candidate and for or against each question by precinct and by groups of precincts, such as districts, wards and countywide.~~	~~M~~	~~The State of Maryland has implemented a process to ensure that COMAR is adhered to for voting system integrity. COMAR requires tabulation and reporting of the total votes cast for each candidate and for or against each question by precinct, and by groups of precincts, such as districts, wards and countywide.~~		
~~T-46~~	~~SBE will ensure that the Election Management System shall tabulate and report total~~	~~M~~	~~SBE has implemented a Logic and Accuracy Test to ensure that COMAR is adhered to for voting system integrity~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	votes cast in each contest and write-in voting positions.		and for each contest and write-in voting positions.		
T-47	SBE will ensure that local election boards conduct, as part of the pre-election testing, a public demonstration, as described in COMAR 33.10.02.16 .	M	The LBE has implemented a public demonstration to ensure that COMAR 33.10.02.16 is met.		

APPENDIX A: ACRONYMS

The following table contains acronyms used in the AccuVote-TS risk assessment report.

ACRONYM	MEANING
ACL	Access Control Lists
C&A	Certification and Accreditation
CIO	Chief Information Officer
COMAR	Code of Maryland Regulations
COOP	Continuity of Operations
DES	Data Encryption Standard
DoS	Denial of Service
DNS	Domain Name Server
DR	Disaster Recovery
DRE	Direct Recording Equipment
EMS	Election Management System
FEC	Federal Election Commission
GSS	General Support System
IDS	Intrusion detection system
IT	Information Technology
ITA	Independent Testing Authority
LBE	Local Board of Elections
NIST	National Institute of Standards and Technology
POC	Point of Contact
RA	Risk Assessment

ACRONYM	MEANING
SAIC	Science Applications International Corporation
SBE	State Board of Elections
ST&E	Security Test and Evaluation
UPS	Uninterrupted Power Source
WAN	Wide Area Network

APPENDIX B: SECURITY STATEMENTS FROM THE RUBIN REPORT & STATE OF MARYLAND CONTROLS

The following table is a brief analysis of statements made by Professor Rubin, et al, in their report on the Diebold source code entitled "Analysis of an Electronic Voting System", July 23, 2003. In general, SAIC made many of the same observations, *when considering only the source code.* While many of the statements made by Mr. Rubin were technically correct, it is clear that Mr. Rubin did not have a complete understanding of the State of Maryland's implementation of the AccuVote-TS voting system, and the election process controls or environment. During this assessment, SAIC had access to system and election documentation, personnel and equipment. Applying the NIST Risk Assessment methodology to the evaluation of the equipment in its operational environment and the totality of the management, operational, and technical controls, SAIC reached many different conclusions. Indeed, Professor Rubin states repeatedly in his paper that he does not know how the system operates in an election and he further identifies the assumptions that he used to reach his conclusions. In those cases where these assumptions concerning operational or management controls were incorrect, the resultant conclusions were, unsurprisingly, also incorrect.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
2	*"The anonymity of a voter's ballot must be preserved, both to guarantee the voter's safety when voting against a malevolent candidate, and to guarantee that voters have no evidence that proves which candidates received their votes."*	O-18, 0-19, 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 that system's PCMCIA card they would be able to tie votes back to individuals.~~
2	*"The voting system must also be tamper-resistant to thwart a wide range of attacks, including ballot stuffing by voters and incorrect tallying by insiders."*	M-4, M-5, O-91	The AccuVote-TS voting system only allows a voter to cast their vote one time. After the individual votes, the Voter Access Card is deactivated. In addition, there are physical, and procedural controls at the polling stations to ensure that voters are only given access to the DRE one time and to make sure that they do not vote multiple times. In addition, when the vote is cast by the voter, the Voter Access Card automatically ejects making a loud noise and the DRE is

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
			disabled until another valid Voter Access Card is inserted.
2	*"A voting system must be comprehensible and usable by the entire voting population, regardless of age, infirmity, or disability."*	N/A	This is not a security requirement.
2	*"The only known solution to this problem is to introduce a "voter-verifiable audit trail." [DMNW03]. Most commonly, this is achieved by adding a printer to the voting terminal. When the voter finishes selecting candidates, a ballot is printed on paper and presented to the voter. If the printed ballot reflects the voter's intent, the ballot is saved for future reference. If not, the ballot is mechanically destroyed. Using this "Mercuri method," [Mer00] the tally of the paper ballots takes precedence over any electronic tallies. As a result, the correctness of the voting terminal software no longer matters; either a voting terminal prints correct ballots or it is taken out of service."*	M-1, M-18, M-90, O-40	The AccuVote-TS voting system requires that the voter verify their selections prior to the actual casting of the vote. This is done via a review screen on the DRE. The AccuVote-TS voting system does not provide a paper "voter-verifiable audit trail" specific to individual voters. Note: A printed paper ballot would still be subject to fraud. A compromised machine could be programmed to record votes incorrectly, but provide a correct paper ballot to the voter. Only in the event of a total recount would this be discovered. Additionally, the process of hand counting the millions of votes is time consuming and is prone to error.
4	*"Most notably, voters can easily program their own smartcards to simulate the behavior of valid smartcards used in the election."*	M-1, M-5, M-83, O-91	Although it is possible for someone to buy and to program their own smartcard, the attacker would be limited to changing their party affiliation in the case of a primary (i.e., they could see a ballot meant for another party) because the smartcard only contains party affiliation and access to vote on the DRE. The combination of logic controls in the DRE software, the physical controls and the openness of the voting booths minimize the likelihood of the voter being able to cast multiple votes without being detected.
4	*"With such homebrew cards, a voter can cast multiple ballots without leaving any trace."*	M-1, M-5, O-91	Although it is possible for someone to buy and to program their own smartcard, the attacker would be limited to changing their party affiliation in the case of a primary (i.e., they could see a ballot meant for another party) because the smartcard only contains party affiliation and access to vote on the DRE. The combination of logic controls in the DRE software, the physical controls and the openness of the voting booths minimize the likelihood of the voter being able

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
			to cast multiple votes without being detected.
4	*"A voter can also perform actions that normally require administrative privileges, including viewing partial results and terminating the election early."*	M-88, O-12, O-14, 0-91,	A voter would need to manufacture a smartcard with administrator rights to obtain these privileges. Assuming someone could manufacture the card and obtained access to the DRE, the specific DRE device could be disabled (i.e., close election). Such an attack would be detected due to the physical controls and the openness of the voting booths. The Disaster Recovery and Incident Management Plan guide provides procedures for handling a disabled DRE.
4	*"Similar undesirable modifications could be made by malevolent poll workers (or even maintenance staff) with access to the voting terminals before the start of an election."*	M-1, M-13, M-26, O-37	The physical controls prevent any single individual from having access to the DRE devices prior to the election. The DRE devices are tested at the LBE warehouse, then 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.
4	*"Furthermore, the protocols used when the voting terminals communicate with their home base, both to fetch election configuration information and to report final election results, do not use cryptographic techniques to authenticate the remote end of the connection nor do they check the integrity of the data in transit."*	M-18, M-41, O-14	The AccuVote-TS voting system is not using a modem to fetch election information. The results of the election however are transmitted. These transmissions are not encrypted. SAIC has recommended that these transmissions be encrypted and that a 100% verification of the transmissions and the PCMCIA cards occur.
4	*"Given that these voting terminals could communicate over insecure phone lines or even wireless Internet connections, even unsophisticated attackers can perform untraceable "man-in-the-middle" attacks."*	N/A	The DRE devices are not connected to a network. The DRE Accumulator is connected via modem after the election to transmit vote totals to the LBE. These transmissions are not encrypted and could be intercepted or modified. SAIC has recommended that these transmissions be encrypted and that a 100% verification of the transmissions and the PCMCIA cards occur.
4	*"Cryptography, when used at all, is used incorrectly."*	M-41, M-124, T-42	Currently, ~~DES~~ encryption is only used for the resident memory on the DRE in accordance with Federal requirements. Once the DRE is powered down, the resident memory is erased. SAIC has recommended that encryption

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
			be employed for the modem transmission of the vote totals.
4	*"In many places where cryptography would seem obvious and necessary, none is used."*	M-41, M-124, T-42	Currently, ~~DES~~ encryption is only used for the resident memory on the DRE. Once the DRE is powered down, the memory is erased. SAIC has recommended that encryption be employed for the modem transmission of the vote totals.
4	*"More generally, we see no evidence of rigorous software engineering discipline. Comments in the code and the revision change logs indicate the engineers were aware of areas in the system that needed improvement, though these comments only address specific problems with the code and not with the design itself."*	M-102, O-72, T-6	The scope of the risk assessment did not include a review of Diebold's software engineering practices. SAIC's review of the source code also noted similar comments. 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.
4	*"We also saw no evidence of any change control process that might restrict a developer's ability to insert arbitrary patches to the code."*	M-102, O-72, T-6	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. SBE and LBE's Logic & Accuracy tests verify that votes are recorded accurately prior to the use of the DRE for any election. SAIC has also recommended that SBE enhance the controls for certifying that the implemented source code is the same version as that certified by the ITA, and to expand their testing to include testing for time-oriented exploits (e.g., trojans). This may be accomplished by changing the machine date and time to correspond to that of the election during testing.
4	*"Absent such processes, a malevolent developer could easily make changes to the code that would create vulnerabilities to be later exploited on Election Day."*	M-10, O-72, T-6	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. SBE and LBE's Logic & Accuracy tests verify that votes are

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
			recorded accurately prior to the use of the DRE for any election. We have also recommended that SBE enhance the controls for certifying that the implemented source code is the same version as that certified by the ITA and to expand their testing to include testing for time-oriented exploits (e.g., trojans). This may be accomplished by changing the machine date and time to correspond to that of the election during testing.
4	*"We also note that the software is written entirely in C++. When programming in an unsafe language like C++, programmers must exercise tight discipline to prevent their programs from being vulnerable to buffer overflow attacks and other weaknesses."*	M-1, M-5, O-34	The scope of the risk assessment did not include a review of Diebold's software engineering practices or an evaluation of which software language may be more secure. Our review did note vulnerabilities that point to software inconsistencies and problems. SBE and LBE's Logic & Accuracy tests verify that votes are recorded accurately prior to the use of the DRE for any election. We have also recommended that SBE enhance the controls for certifying that the implemented source code is the same version as that certified by the ITA and to expand their testing to include testing for time-oriented exploits (e.g., trojans). This may be accomplished by changing the machine date and time to correspond to that of the election during testing.
4	*"Indeed, buffer overflows caused real problems for AccuVote-TS systems in real elections."* (Note: This reference has nothing to do with buffer overflows)	N/A	It is true that this system is not configured to defend against buffer overflow attacks. As the DRE has no network connections, an attacker is not provided a means to exploit this vulnerability.
4	*"Although the Diebold code is designed to run on a DRE device (an example of which is shown in Figure 1), one can run it on a regular Microsoft Windows computer (during our experiments we compiled and ran the code on a Windows 2000 PC)."*	N/A	This is not a security requirement.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
4	*"In the following we describe the process for setting up and running an election using the Diebold system. Although we know exactly how the code works from our analysis, we must still make some assumptions about the external processes at election sites. In all such cases, our assumptions are based on the way the Diebold code works, and we believe that our assumptions are reasonable. There may, however, be additional administrative procedures in place that are not indicated by the source code."*	N/A	This is not a security requirement, but it does give insight into the methodology used by the Rubin team in the drafting the report.
5	*"In common usage, we believe the voting terminals will be distributed without a ballot definition pre-installed."*	M-7, M-10, O-8	This assumption is invalid. The voting terminals are distributed with the state approved ballot information loaded.
5	*"We do not know exactly how the voter gets his voter card. It could be sent in the mail with information about where to vote, or it could be given out at the voting site on the day of the election. To understand the voting software itself, however, we do not need to know what process is used to distribute the cards to voters."*	O-103	This assumption is invalid. The Voter Access Cards are distributed at the polling site after the voter is vetted, and retrieved from the voter after the voter has cast their vote.
5	*"As we have only analyzed the code for the Diebold voting terminal, we do not know exactly how the back-end server tabulates the final results it gathers from the individual terminals. Obviously, it collects all the votes from the various voting terminals. We are unable to verify that there are checks to ensure, for example, that there are no more votes collected than people who are registered at or have entered any given polling location."*	M-1, M-5, O-16, O-91	SBE and LBEs have numerous checks and balances to ensure that the votes entered on the DRE devices are accurately reported. There are checks at the polling site, the LBE HQ and SBE. SAIC has recommended that the checks and balances be augmented to include a 100% verification of the vote transmissions to the PCMCIA cards.
9	*"Upon reviewing the Diebold code, we observed that the smartcards do not perform any cryptographic operations."*	NA	That is correct, the smartcards perform no cryptographic functions. The smartcards also do not contain any sensitive or personal information. The smartcards contain party affiliation (in the case of a primary election) and access to vote on the DRE.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
9	*"For example, authentication of the terminal to the smartcard is done "the old-fashioned way:" the terminal sends a clear text (i.e., unencrypted) 8-byte password to the card and, if the password is correct, the card believes that it is talking to a legitimate voting terminal. Unfortunately, this method of authentication is insecure: an attacker can easily learn the 8-byte password used to authenticate the terminal to the card (see Section 3.3), and thereby communicate with a legitimate smartcard using his own smartcard reader."*	M-5, M-83, M-124, O-12, O-15, O-36, O-92,	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 attach a card reader to the voting terminal would be easily visible to any of the many election officials. In addition, the vetting process limits access to DRE devices to eligible voters.
9	*"Furthermore, there is no authentication of the smartcard to the device. This means that nothing prevents an attacker from using his own homebrew smartcard in a voting terminal."*	M-5, M-83, O-12, O-15, O-36, O-92	Although it is possible for someone to buy and to program their own smartcard, the attacker would be limited to changing their party affiliation in the case of a primary (i.e., they could see a ballot meant for another party) because the smartcard only contains party affiliation and access to vote on the DRE. The combination of logic controls in the DRE software, the physical controls and the openness of the voting booths minimize the likelihood of the voter being able to cast multiple votes without being detected.
9	*"An attacker who knows the protocol spoken by the voting terminal to the legitimate smartcard could easily implement a homebrew card that speaks the same protocol."*	M-5, M-83, O-12, O-15, O-36, O-91, O-92,	Although it is possible for someone to buy and to program their own smartcard, the attacker would be limited to changing their party affiliation in the case of a primary (i.e., they could see a ballot meant for another party) because the smartcard only contains party affiliation and access to vote on the DRE. The combination of logic controls in the DRE software, the physical controls and the openness of the voting booths minimize the likelihood of the voter being able to cast multiple votes without being detected.
9	*"Even if the attacker does not a priori know the protocol, an attacker could easily learn enough about the protocol to create new voter cards by attaching a "wiretap" device between the voting terminal and a legitimate smartcard and observing the communicated messages."*	M-5, M-83, O-12, O-15, O-36, O-92	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 attach a card reader to the voting terminal would be easily visible to any of the many election officials. In addition, the vetting process limits access to DRE devices to eligible voters.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
			limits access to DRE devices to eligible voters.
9	*"The parts for building such a device are readily available and, given the privacy of voting booths, might be unlikely to be noticed by poll workers. An attacker might not even need to use a wiretap to see the protocol in use."*	M-5, O-12, O-36	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 attach a card reader to the voting terminal would be easily visible to any of the many election officials.
9	*"Likewise, the important data on the legitimate voting card is stored as a file (named 0x3D40 — smartcard files have numbers instead of textual file name) that can be easily read by a portable smartcard reader. Again, given the privacy of voting booths, an attacker using such a card reader would be unlikely to be noticed. Given the ease with which an attacker can interact with legitimate smartcards, plus the weak password-based authentication scheme (see Section 3.3), an attacker could quickly gain enough insight to create homebrew voting cards, perhaps quickly enough to be able to use such homebrew cards during the same election day."*	M-5, O-91	The privacy of the voting booth is limited. If one pictures the old, curtained voting booths of the past, this could be possible. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to attach a card reader to the voting terminal would be easily visible to any of the many election officials.
9	*"The only impediment to the mass production of homebrew smartcards is that each voting terminal will make sure that the smartcard has encoded in it the correct m_ElectionKey, m_VCenter, and m_DLVersion (see DoVote() in BallotStation/Vote.cpp). The m_ElectionKey and m_DLVersion are likely the same for all locations and, furthermore, for backward-compatibility purposes it is possible to use a card with m_ElectionKey and m_DLVersion undefined. The m_VCenter value could be learned on a per-location-basis by interacting with legitimate smartcards, from an insider, or from inferences based on the m_VCenter values observed at other polling locations."*	M-16, M-17, M-32, O-4, O-12, O-14	Although it is possible for someone to buy and to program their own smartcard, the attacker would be limited to changing their party affiliation in the case of a primary (i.e., they could see a ballot meant for another party) because the smartcard only contains party affiliation and access to vote on the DRE. The combination of logic controls in the DRE software, the physical controls and the openness of the voting booths minimize the likelihood of the voter being able to cast multiple votes without being detected.
10	*"Since an adversary can make perfectly valid smartcards, the adversary could bring a stack of active cards to the*	M-83, 112, M-113, O-	The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	voting booth. Doing so gives the adversary the ability to vote multiple times."	91	the voter's selections. The action of trying to run numerous smartcards through the voting terminal would be easily visible to any of the many election officials. In addition, the voting machine makes a loud noise and ejects the smartcard after each vote is cast.
10	*"More simply, instead of bringing multiple cards to the voting booth, the adversary could program a smartcard to ignore the voting terminal's deactivation command. Such an adversary could use one card to vote multiple times."*	M-83, M-88, M-113, O-91	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 cast multiple votes would be easily visible to any of the many election officials. Additionally, there are procedures to ensure that only the correct number of votes have been cast on each DRE. Each polling site checks the number of Voter Authority Cards signed, to the register, then to the total votes cast on DREs.
10	*"Will the adversary's multiple-votes be detected by the voting system? To answer this question, we must first consider what information is encoded on the voter cards on a per-voter basis. The only per-voter information is a "voter serial number" (m_VoterSN in the CVoterInfo class). Because of the way the Diebold system works, m_VoterSN is only recorded by the voting terminal if the voter decides not to place a vote (as noted in the comments in TSElection/Results.cpp, this field is recorded for uncounted votes for backward compatibility reasons). It is important to note that if a voter decides to cancel his or her vote, the voter will have the opportunity to vote again using that same card (and, after the vote has been cast, m_VoterSN will not be recorded)."*	M-9, M-132, M-136, M-142	There are procedures to ensure that only the correct number of votes have been cast on each DRE. Each polling site checks the number of Voter Authority Cards signed, to the register, then to the total votes cast on DREs.
10	*"Can the back-end tabulation system detect multiple-vote casting? If we assume the number of collected votes becomes greater than the number of people who showed up to vote, and if the polling locations keep accurate counts of the number of people who show up to vote, then the back-end system, if designed properly, should be able*	M-9, M-132, M-136, M-142, O-91	As noted, Mr. Rubin did not look at the backend tabulating system. SBE and LBE have numerous checks and balances to ensure that the votes entered on the DRE devices are accurately reported. There are checks at the polling site, the LBE HQ and SBE. SAIC has recommended that the checks and balances be augmented to include a

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	to detect the existence of counterfeit votes. However, because m_VoterSN is only stored for those who did not vote, there will be no way for the tabulating system to count the true number of voters or distinguish the real votes from the counterfeit votes. This would cast serious doubt on the validity of the election results. We point out, however, that we only analyzed the voting terminal's code; we do not know whether such checks are performed in the actual back-end tabulating system."		100% verification of the vote transmissions to the PCMCIA cards.
10	*"Just as an adversary can manufacture his or her own voter cards, an adversary can manufacture his or her own administrator and ender cards (administrator cards have an easily-circumventable PIN, which we will discuss in Section 3.2). This attack is easiest if the attacker has knowledge of the Diebold code or can interact with a legitimate administrator or ender card."*	M-83, O-4, O-12	Assuming someone could manufacture the card and obtained access to the DRE, the specific DRE device could be disabled (i.e., close election). Such an attack would be detected due to the physical controls and the openness of the voting booths. The Disaster Recovery and Incident Management Plan guide provides procedures for handling a disabled DRE.
10	*"Using a homebrew administrator card, a poll worker, who might not otherwise have access to the administrator functions of the Diebold system but who does have access to the voting machines before and after the elections, could gain access to the administrator controls. If a malicious voter entered an administrator or ender card into the voting device instead of the normal voter card, then the voter would be 10 able to terminate the election and, if the card is an administrator card, gain access to additional administrative controls."*	M-1, M-13, O-4, O-12, O-14, O-17	Assuming someone could manufacture the card and obtained access to the DRE, the specific DRE device could be disabled (i.e., close election). Such an attack would be detected due to the physical controls and the openness of the voting booths. The Disaster Recovery and Incident Management Plan guide provides procedures for handling a disabled DRE.
11	*"The use of administrator or ender cards prior to the completion of the actual election represents an interesting*	M-1, M-5, M-83, M-	Assuming someone could manufacture the card and obtained access to the DRE, the specific DRE device could

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	completion of the actual election represents an interesting denial-of-service attack. Once "ended," the voting terminal will no longer accept new voters (see CVoteDlg::OnCardIn()) until the terminal is somehow reset. Such an attack, if mounted simultaneously by multiple people, could shut down a polling place. If a polling place is in a precinct considered to favor one candidate over another, attacking that specific polling place could benefit the less-favored candidate. Even if the poll workers were later able to resurrect the systems, the attack might succeed in deterring a large number of potential voters from voting (e.g., if the attack was performed over the lunch hour). If such an attack was mounted, one might think the attackers would be identified and caught. We note that many governmental entities do not require identification to be presented by a voter, instead allowing for "provisional" ballots to be cast. By the time the poll workers realize that one of their voting terminals has been disabled, the perpetrator may have long-since left the scene."	M-83, M-88, M-91, M-113, O-4, O-14, O-22	obtained access to the DRE, the specific DRE device could be disabled (i.e., close election). Such an attack would be detected due to the physical controls and the openness of the voting booths. The Disaster Recovery and Incident Management Plan guide provides procedures for handling a disabled DRE. If as suggested, multiple individuals mounted a simultaneous attack at a polling site, with forged administrator cards, and closed the DRE devices, and we assume that they all successfully got away, the Election Judges still could immediately reopen the DRE devices. The Disaster Recovery and Incident Management Plan guide provides procedures for handling a disabled DRE.
11	*"Upon looking more closely at this administrator authentication process, however, we see that there is a flaw with the way the PINs are verified. When the terminal and the smartcard first begin communicating, the PIN value stored on the card is sent in cleartext from the card to the voting terminal. Then, when the user enters the PIN into the terminal, it is compared with the PIN that the smartcard sent (CPinDlg::OnOK()). If these values are equal, the system accepts the PIN. Herein lies the flaw with this design: any person with a smartcard reader can easily extract the PIN from an administrator card. The adversary doesn't even need to fully understand the protocol between the terminal and the device: if the response from the card is n bytes long, the attacker who correctly guesses that the PIN is sent in the clear would only have to try n¡3 possible PINs, rather than 10,000. This*	M-1, M-5, O-4, O-14	Assuming someone could manufacture the card and obtained access to the DRE or obtained a valid administrator's card and PIN combinations, the specific DRE device could be disabled (i.e., close election). Such an attack would be detected due to the physical controls and the openness of the voting booths. The Disaster Recovery and Incident Management Plan guide provides procedures for handling a disabled DRE. Additionally the privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	means that the PINs are easily circumventable. Of course, if the adversary knows the protocol between the card and the device, an adversary could just make his own administrator card, using any desired PIN (Section 3.1.2)."		
12	*"There are several issues with the above code. First, hard-coding passwords in C++ files is generally a poor design choice. We will discuss coding practices in more detail in Section 6, but we summarize some issues here. Hard-coding passwords into C++ files suggests a lack of key and password management."*	M-111	Hard-coding of passwords is not consistent with best security practice. We have recommended that the hard-coded passwords be removed and changed.
12	*"Furthermore, even if the developers assumed that the passwords would be manually changed and the software recompiled on a per-election basis, it would be very easy for someone to forget to change the constants in VoterCard/CLXSmartCard.cpp. (Recompiling on a per-election basis may also be a concern, since good software engineering practices would dictate additional testing and certification if the code were to be recompiled for each election.)"*	M-1, M-5, M-111	This assumption is invalid assumption. The software is not recompiled on a per-election basis. In addition, only source code certified by the ITA is loaded on the devices. SBE and LBE's Logic & Accuracy tests verify that votes are recorded accurately. SAIC has recommended that SBE enhance the controls for certifying that the implemented source code is the same verison as that certified by the ITA and to expand their testing to include testing for time-oriented exploits (e.g., trojans). This may be accomplished by changing the machine date and time to correspond to that of the election during testing.
12	*"The above issues would only be a concern if the authentication method were otherwise secure. Unfortunately, it is not. Since the password is sent in the clear from the terminal to the card, an attacker who puts a fake card into the terminal and records the command from the terminal will be able to learn the password (and file name) and then re-use that password with real cards. An adversary with knowledge of this password could then create counterfeit voting cards. As we have already discussed (see Section 3.1.1), this can allow the adversary to cast multiple votes, among other attacks. Hence, the authentication of the voting terminal to the smartcards is*	M-1, M-5, M-95, M-111, M-112, O-12, O-35	The smartcard allows the voter to enter a vote, but the user is authenticated during the vetting process, (i.e., the control over who gets to vote is not controlled by the smartcard, but by the vetting procedures). Once again 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 cast multiple votes would be easily visible to any of the many election officials. In addition, the voting machine makes a loud noise and ejects the smartcard after each vote is cast.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	insecure."		
12	*"Furthermore, note the control flow in the above code-snippet. If the password chosen by the designers of the system ("\xED\x0A\xED\x0A\xED\x0A\xED\x0A") does not work, then CCLXSmartCard::* *Open() uses the smartcard manufacturer's default password of "\x00\x01\x02\x03\x04\x05\x06\x07."* *One issue with this is that it implies that sometimes the system is used with un-initialized smartcards. This means that an attacker might not even need to figure out the system's password in order to be able to authenticate to the cards."*	M-83, M-86	The smartcard allows the voter to enter vote, but the user is authenticated during the vetting process, (i.e., the control over who gets to vote is not controlled by the smartcard, but by the vetting procedures). In addition, once again 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 cast multiple votes would be easily visible to any of the many election officials. In addition, the voting machine makes a loud noise and ejects the smartcard after each vote is cast.
12	*"As we noted in Section 3.1, some smartcards allow a user to get a listing of all the files on a card. If the system uses such a card and also uses the manufacturer's default password of \x00\x01\x02\x03\x04\x05\x06\x07, then an attacker, even without any knowledge of the source code and without the ability to intercept the connection between a legitimate card and a voting terminal, but with access to a legitimate voter card, will still be able to learn enough about the smartcards to be able to create counterfeit voter cards."*	M-83, M-88	The smartcard allows the voter to enter vote, but the user is authenticated during the vetting process, (i.e., the control over who gets to vote is not controlled by the smartcard, but by the vetting procedures). Once again 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 cast multiple votes would be easily visible to any of the many election officials. In addition, the voting machine makes a loud noise and ejects the smartcard after each vote is cast.
13	*"Unfortunately, under Windows CE, which we believe is used in commercial Diebold voting terminals, the existence of the removable storage device is not enforced properly."*	M-5	The PCMCIA cards are locked into the DRE device. The key is controlled by the Chief Judges. Additionally, we have recommended that the State further secure this locked compartment using tamper-proof tape during the actual election
13	*"Unlike other versions of Windows, removable storage cards are mounted as subdirectories under CE. When the voting software wants to know if a storage card is inserted, it simply checks to see if the Storage Card subdirectory*	M-83, M-112, M-113	Pre-election Logic and Accuracy testing checks both the main storage area, and the removable memory.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	exists in the filesystem's root directory. While this is the default name for a mounted storage device, it is also a perfectly legitimate directory name for a directory in the main storage area. Thus, if such a directory exists, the terminal can be fooled into using the same storage device for all of the data. This would reduce the amount of redundancy in the voting system and would increase the chances that a hardware fault could cause recorded votes to be lost."		
13	*"The majority of the system configuration information for each terminal is stored in the Windows registry under HKEY_LOCAL_MACHINE\Software\GlobalElectionSystems\AccuVote-TS4 . This includes both identification information such as the terminal's serial number and more traditional configuration information such as the COM port that the smartcard reader is attached to. All of the configuration information is stored in the clear, without any form of integrity protection. Thus, all an adversary must do is modify the system registry to trick a given voting terminal into effectively impersonating any other voting terminal."*	M-83, M-112, M-113, M-120, O-12, O-17, O-35	Exploitation of this vulnerability requires access to the system registry. Since the DRE is not connected to a network, an attacker's access to the registry is limited by procedural and physical barriers.
13	*"It is unclear how the tallying authority would deal with results from two different voting terminals with the same voting ID — at the very least human intervention to resolve the conflict would probably be required."*	M-1, M-5	Prior to each election, the GEMS server assigns a unique number to each PCMCIA card as part of the ballot loading process. When the results are read from the PCMCIA cards at the conclusion of the election, the GEMS server uses this unique number to validate acceptance of the data. If two of these numbers are identical, the election officials would investigate using established procedures.
13	*"The Federal Election Commission draft standard requires each terminal to keep track of the total number of votes that have ever been cast on it — the "Protective Counter." This counter is used to provide yet another method for ensuring that the number of votes cast on each terminal is correct. However, as the following code from*	M-121, M-167, O-7, O-96, T-11	This exploit requires access to the system. Since the system is not connected to a network, physical access is required. 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

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	Utilities/machine.cpp shows, the counter is simply stored as an integer in the file system.bin in the terminal's system directory (error handling code has been removed for clarity): *long GetProtectedCounter()* *{* *DWORD protectedCounter = 0;* *CString filename = ::GetSysDir();* *filename += _T("system.bin");* *CFile file;* *file.Open(filename, CFile::modeRead | CFile::modeCreate |* *CFile::modeNoTruncate);* *file.Read(&protectedCounter, sizeof(protectedCounter));* *file.Close();* *return protectedCounter;* *}* *By modifying this counter, an adversary could cast doubt on an election by creating a discrepancy between the number of votes cast on a given terminal and the number of votes that are tallied in the election. While the current method of implementing the counter is totally insecure, even a cryptographic checksum would not be enough to*		of the many election officials. Other physical and procedural controls are effective in preventing access to the system prior to, or after an election.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	protect the counter; an adversary with the ability to modify and view the counter would still be able to roll it back to a previous state. In fact, the only solution that would work would be to implement the protective counter in a tamper-resistant hardware token, requiring modifications to the physical voting terminal hardware."		
14	*"The "ballot definition" for each election contains everything from the background color of the screen to the PPP username and password to use when reporting the results. This data is not encrypted or check summed (cryptographically or otherwise) and so can be easily modified by any attacker with physical access to the file."*	M-7, M-8, M-10, O-14	As stated, this assumption requires access to the system. Since the system is not connected to a network, physical access is required. 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 DRE would be easily visible to any of the many election officials.
14	*"By simply changing the order of the candidates as they appear in the ballot definition, the results file will change accordingly. However, the candidate information itself is not stored in the results file. The file merely tracks that candidate 1 got so many votes and candidate 2 got so many other votes. If an attacker reordered the candidates on the ballot definition, voters would unwittingly cast their ballots for the wrong candidate. As with denial-of-service attacks (see Section 3.1.2), ballot reordering attacks would be particularly effective in polling locations known to be heavily partisan."*	M-7, M-8, O-3, O-14	This exploit requires access to the system. Since the system is not connected to a network, physical access is required. 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. In addition, the ballot is on the PCMCIA card, which is locked in the DRE device. Note: SBE uses a public FTE site to distribute ballot information. While there are many checks at the LBE of the ballot, SAIC has recommended that SBE implement a secure method to transfer the ballot.
14	*"Even without modifying the ballot definition, an attacker can gain almost enough information to impersonate the voting terminal to the back-end server. The terminal's voting center ID, PPP dial-in number, username, password and the IP address of the back-end server are all available in the clear (these are parsed into a CElectionHeaderItem in TSElection\TSElectionObj.cpp). Assuming an attacker is able to guess or create a voting terminal ID, he would be*	M-5; M-14, M-39, O-23	The LBE GEMS server (i.e., backend server) is not connected to a network. The LBE GEMS server checks for PCMCIA cards from the modem transmissions. This error checking accounts both for card validity (i.e. that the card was issued and is not a duplicate) and ensures that all issued cards are reported. SAIC has recommended that the modem transmissions be