Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	actions.		server administrator guide describes audit trail mechanisms on the server side.		
M-133	System security planning should address if the audit trails support after-the-fact investigations of how, when, and why normal operations ceased.	U	If system security planning does not address if the audit trails support after-the-fact investigations of how, when, and why normal operations ceased, then audit trails may be incomplete and the confidentiality, integrity, and availability of the system may be compromised. There is no documentation requiring the review of audit trails. Without regular event log review, it is very difficult to identify when any improper use of the system has occurred. **Likelihood: HIGH** Without regular audit log reviews, intrusion or intrusion attempts could go undetected. **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.	**HIGH**	A formal and documented process requiring the review of audit logs should be implemented.
M-134	System security planning should address if the audit trails are designed and implemented	U	If system security planning does not address if the audit trails are designed and implemented to record appropriate	**HIGH**	Implement a formal and documented process describing the proper configuration of audit trails.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	to record appropriate information that can assist in intrusion detection.		information that can assist in intrusion detection, then audit trails may be incomplete and the confidentiality, integrity, and availability of the system may be compromised. There is no documentation describing the required configuration of audit trails to record information to assist in intrusion detection. **Likelihood: HIGH** Without this documentation, the application of the audit security control may be applied inconsistently, incorrectly, or incompletely. **Impact: HIGH** Both intentional and unintentional human threats can cause damage to the system. Without proper audit log configuration and periodic audit log review, inappropriate system activity may not be detected. Exercise of this vulnerability could result in significant impairment to the SBE mission.		configuration of audit trails.
M-135	System security planning should address if the audit trails are used as online tools to help identify problems other than intrusions as they occur.	U	If system security planning does not address if the audit trails are used as online tools to help identify problems other than intrusions as they occur, then problems other than intrusions may go undetected or unresolved and the confidentiality, integrity, and availability	LOW	Consider documenting and implementing the use of online audit tools for identifying system problems, if cost effective.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			of the system may be compromised. There is no documentation addressing if the audit trails are used as online tools to help identify problems as they occur. Without online event log review, it is difficult to identify problems as they occur. **Likelihood: HIGH** There are no online event logs available on the server for review. **Impact: LOW** Because online event logs are not available to assist in problem identification, problem resolution may take longer to accomplish.		
M-136	System security planning should address if audit trails specify type of event, when the event occurred, user ID associated with the event, and program or command used to initiate the event.	U	If system security planning does not address if audit trails specify type of event, when the event occurred, user ID associated with the event, and program or command used to initiate the event, then audit trails may be incomplete and the confidentiality, integrity, and availability of the system may be compromised. There is no documentation to specify type of event, when the event occurred, user ID associated with the event, and program or command used to initiate the event. Without the ability to associate users with events accountability cannot	HIGH	Implement a formal and documented process describing the proper configuration of audit trails, specify the type of events to audit, when the event occurred, user ID associated with the event, and program or command used to initiate the event.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			be enforced. **Likelihood: HIGH** Without properly configured audit logs that are reviewed regularly, individual accountability for system actions can not be enforced. **Impact: HIGH** Both intentional and unintentional human threats can cause damage to the system. Without proper audit log configuration and periodic audit log review, inappropriate system activity may not be detected. Exercise of this vulnerability could result in significant impairment to the SBE mission.		
M-137	System security planning should address if access to electronic audit logs is strictly controlled.	U	If system security planning does not address if access to electronic audit logs is strictly controlled, then unauthorized access to electronic logs may occur resulting in the loss of audit trails and the confidentiality, integrity, and availability of the system may be compromised. There is no documentation addressing if access to electronic audit logs is strictly controlled. Without controlling access to the logs, they may be deleted either intentionally or unintentionally. **Likelihood: LOW** Other processes and controls, including	**LOW**	Implement a formal and documented process addressing access to electronic audit logs.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			physical isolation and small number of privileged users, reduces the likelihood of exploiting this vulnerability. **Impact: HIGH** If the audit logs are improperly modified or deleted, accountability for user actions cannot be enforced.		
M-138	System security planning should address if there exists separation of duties between security personnel who administer the access control function and those who administer the audit trail.	P	If system security planning does not address if there exists separation of duties between security personnel who administer the access control function and those who administer the audit trail, then a conflict of interest may exist whereby the audit trail can be circumvented resulting in the potential compromise of system confidentiality, integrity, and availability. Separation of Duties is practiced when possible due to the lack of resources at the SBE and LBEs, so most often the system administrator conducts both duties. **Likelihood: HIGH** A malicious administrator can exploit this vulnerability. **Impact: MEDIUM** Inappropriate activity may not be detected and losses may occur through a malicious administrator adding	**MEDIUM**	Implement a formal and documented process addressing how Separation of Duties is to be implemented.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			inappropriate users to the system without being detected.		
M-139	System security planning should address how confidentiality of audit trail information is protected.	U	If system security planning does not address how confidentiality of audit trail information is protected, then unauthorized access or modification to audit trails may occur resulting in the loss of the confidentiality of the audit trail information. There is no documentation addressing how confidentiality of audit trail information is protected. Without security controls implemented to identify fraudulent or erroneous changes to the system, it is difficult to identify when any improper use of the system has occurred, therefore audit trail data should remain confidential. **Likelihood: LOW** Other processes and controls, including physical isolation and small number of privileged users, reduces the likelihood of exploiting this vulnerability. **Impact: HIGH** Both intentional and unintentional human threats can cause damage to the system. Inappropriate activity may not be detected and significant losses may occur.	LOW	Implement a formal and documented process addressing how confidentiality of audit trail information is protected.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
M-140	System security planning should describe how frequently audit trails are reviewed and whether there are review guidelines.	U	If system security planning does not describe how frequently audit trails are reviewed and whether there are review guidelines, then audit trails may not be reviewed in a timely manner resulting in the failure to identify potential threats/vulnerabilities before they are exercised which may eventually lead to the compromise of the system confidentiality, integrity, and availability. There is no documentation describing how frequently audit trails are to be reviewed and there are no review guidelines. Without security controls implemented to identify fraudulent or erroneous changes to the system, it is difficult to identify when any improper use of the system has occurred, therefore audit trail data should remain confidential. **Likelihood: LOW** Other processes and controls, including physical isolation and small number of privileged users, reduces the likelihood of exploiting this vulnerability. **Impact: HIGH** Both intentional and unintentional human threats can cause damage to the system. Inappropriate activity may not be detected and significant losses may occur.	LOW	Implement a formal and documented process describing how frequently audit trails are reviewed.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
~~M-141~~	~~System security planning should address if the audit trails can be queried by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information.~~	~~M~~	~~The system documentation describes the process for reviewing event system logs by application name, date, time, user ID and terminal ID.~~		
~~M-142~~	~~System security planning should address if the appropriate system-level or application-level administrator reviews the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.~~	~~M~~	~~The Technicians Guide, GEMS Server Administrator Guide, and the RISC database describe the appropriate system-level or application-level administrator reviews the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.~~		
~~M-143~~	~~The System security planning should address the use of audit analysis tools.~~	~~U~~	~~If the System security planning does not address the use of audit analysis tools, then the audit analysis tools may be inappropriately used or deployed resulting in the failure to identify potential threats/vulnerabilities before they are exercised which may eventually lead to the compromise of the system confidentiality, integrity, and availability.~~ ~~Documentation does not address the use of audit analysis tools. Analyzing audit logs is a time consuming, labor intensive requirement, therefore audit analysis tools should be used.~~	~~LOW~~	~~Implement a formal and documented process addressing the use of audit analysis tools.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			Likelihood: LOW Other processes and controls, including physical isolation and small number of privileged users, reduces the likelihood of exploiting this vulnerability. **Impact: HIGH** Both intentional and unintentional human threats can cause damage to the system. Inappropriate activity may not be detected and significant losses may occur.		
M-144	Senior Management must assess and incorporate results of the risk assessment activity into the decision making process.	**M**	Results from this risk assessment will determine the effectiveness of existing security controls, provide recommendations, and establish baseline controls. Continue the risk assessment process at least every three years or whenever major changes occur throughout all phases of the system's life cycle.		
M-145	SBE should support or use the risk management process to identify and assess new potential risks and implement new security controls as needed to safeguard their IT systems.	**M**	Results from this risk assessment will determine the effectiveness of existing security controls, provide recommendations, and establish baseline controls. Continue the risk assessment process at least every three years or whenever major changes occur throughout all phases of the system's life cycle.		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~Note: This risk assessment is the first performed on the Accuvote-TS voting system.~~		
~~M-146~~	~~IT security trainers or security/subject matter professionals must understand the risk management process so that they can develop appropriate training materials and incorporate risk assessment into training programs to educate the end users.~~	~~M~~	~~The RISC Plan, SBE and LBE training manuals address the risk management process in regards to the training programs. Future training should place greater emphasis on the risk management process.~~		
~~M-147~~	~~To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system.~~	~~M~~	~~Results from this risk assessment will determine the effectiveness of existing security controls, provide recommendations, identify threats, and establish baseline controls.~~ ~~Note: This risk assessment is the first performed on the Accuvote-TS voting system.~~		
~~M-148~~	~~An estimate of the motivation, resources, and capabilities that may be required to carry out a successful attack should be developed after the potential threat-sources have been identified, in order to determine the likelihood of a threat exercising a system vulnerability.~~	~~M~~	~~Results from this risk assessment will determine the effectiveness of existing security controls, provide recommendations, assess threats, and establish baseline controls.~~ ~~Note: This risk assessment is the first performed on the Accuvote-TS voting system.~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
M-149	If the IT system has not yet been designed, the search for vulnerabilities should focus on the organizations security policies, planned security procedures, and system requirement definitions, and the vendors or developers security product analyses.	N/A	The system is not in the design phase.		
M-150	If the IT system is being implemented, the identification of vulnerabilities should be expanded to include more specific information, such as the planned security features described in the security design documentation and the results of system certification test and evaluation.	N/A	The system is not in the implementation phase.		
M-151	If the IT system is operational, the process of identifying vulnerabilities should include an analysis of the IT system security features and the security controls, technical and procedural, used to protect the system.	M	Results from this risk assessment will determine the effectiveness of existing security controls, provide recommendations, identify threats, and establish baseline controls. Note: This risk assessment is the first performed on the Accuvote-TS voting system.		
M-152	A cost-benefit analysis should be conducted for the proposed recommended controls, to demonstrate that the costs of implementing the controls can	M	The SBE RISC Plan addresses proposed recommended controls and provides justification and cost/benefit analysis information.		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~be justified by the reduction in the level of risk.~~				
~~M-153~~	~~The operational impact (e.g., effect on system performance) and feasibility (e.g., technical requirements, user acceptance) of introducing the recommended option should be evaluated carefully during the risk mitigation process.~~	~~M~~	~~The SBE RISC Plan addresses the operational impact and feasibility of introducing the recommended option and provides for careful evaluation during the risk mitigation process.~~		
~~M-154~~	~~Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing.~~	~~M~~	~~This risk assessment documents the risks, effectiveness of existing security controls, provides recommendations, identifies threats, and establishes baseline controls.~~ ~~Note: This risk assessment is the first performed on the Accuvote-TS voting system.~~		
~~M-155~~	~~The goals and mission of an organization should be considered in selecting any risk mitigation options.~~	~~M~~	~~This risk assessment considers the goals and missions of SBE when suggesting risk mitigation options. In addition, the SBE RISC Plan ensures that the controls recommended by this risk assessment consider the goals and mission of the SBE.~~		
~~M-156~~	~~Priority should be given to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm.~~	~~M~~	~~This risk assessment gives priority to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm.~~ ~~Note: This risk assessment is the first performed on the Accuvote-TS voting~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~system.~~		
~~M-157~~	~~Ongoing risk management should be conducted to assess and mitigate risk.~~	~~M~~	~~The SBE RISC Plan ensures ongoing risk management is conducted to assess and mitigate risk.~~		
~~M-158~~	~~IT systems should be authorized to address and accept residual risk.~~	~~M~~	~~The SBE RISC Plan ensures that IT systems are authorized to operate and that residual risk is accepted.~~		
~~M-159~~	~~If the residual risk has not been reduced to an acceptable level, the risk management cycle must be repeated to identify a way of lowering the residual risk to an acceptable level.~~	~~M~~	~~The SBE RISC Plan ensures that residual risk is accepted or lowered to an acceptable level through the risk management cycle.~~		
~~M-160~~	~~There should be a specific schedule for assessing and mitigating mission risks~~	~~M~~	~~The SBE RISC Plan and the Change Control Plan have a specific schedule for accessing and mitigating risks.~~		
~~M-161~~	~~Risk management should identify residual risks for which contingency plans must be put into place.~~	~~M~~	~~The SBE Disaster Recovery and Incident Management Plan details the procedures to recover from a disaster/incident. This risk assessment identifies residual risks for which contingency plans must be put into place.~~		
~~M-162~~	~~SBE shall require that the system design should incorporate redundancy directly into the system architecture to optimize reliability, maintainability, and availability.~~	~~M~~	~~The system specifications incorporate redundancy directly into the system architecture to optimize reliability, maintainability, and availability.~~		
~~M-163~~	~~SBE shall have contingency test plans~~	~~M~~	~~The SBE Disaster Recovery and Incident Management Plan details the procedures~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	test plans.		Management Plan details the procedures for contingency test plans.		
M-164	The contingency plan should be updated to reflect changes to procedures based on lessons learned.	M	The SBE Disaster Recovery and Incident Management Plan and the Configuration Control Plan are updated based on lessons learned.		
M-165	The State Administrator shall maintain management control over the system and all support personnel provided by the system vendor.	M	The State Administrator maintains management control over the system and all support personnel as stated in the COMAR.		
M-166	SBE will ensure that any equipment within the control of a vendor for repairs, the equipment may not be used for voting or any election purposes.	M	The Election Judge manuals, SBE Maintenance Plan and the Election Administration Guide ensure that any equipment within the control of a vendor is not used for voting or any election purposes.		
M-167	Votes shall be recorded in audit trail memory, both in the voting unit and on the memory card, in two formats: as a summary total for each candidate and question, and as an individual ballot image of each voter's selection.	M	This voting system is compliant FEC standards. Votes are recorded in audit trail memory, both in the voting unit and on the memory card, in two formats: as a summary total for each candidate and question, and as an individual ballot image of each voter's selection as stated in the vendor guides.		
M-168	During post voting verification, if the verification does not agree with the original tabulation, the local board shall immediately notify the State Administrator.	M	As directed in COMAR, Election Administrators Guide and the Official Canvassing Guide local board shall immediately notify the State Administrator if the verification does not agree with the original tabulation.		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
M-169	The system and its components will only be used for conducting elections and may not be used for any other purpose.	M	The system and its components are only used for conducting elections and not used for any other purpose.		

Operational Controls

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
O-1	SBE will test electronic voting equipment for the proper implementation of state-specific requirements.	M	The SBE has User Acceptance Testing Guidelines in place to perform acceptance testing on all electronic voting equipment and UPS devices against state requirements. The SBE and LBE have AccuVote-TS Logic & Accuracy Testing in place to test the electronic voting equipment meets state requirements.		
O-2	SBE will define user acceptance testing for all electronic voting equipment.	M	The SBE has User Acceptance Testing Guidelines in place to perform acceptance testing on all electronic voting equipment and UPS devices against state requirements.		
O-3	SBE will ensure that a process is implemented that ensures that all voting devices shall record and retain redundant copies of the original ballot image.	M	SBE requires ITA certification, which ensures that all voting devices shall record and retain redundant copies of the original ballot image.		
O-4	SBE will ensure that a process is implement that protects against a single point of failure that would prevent further voting at the polling place.	M	The Election Judge manuals, AccuVote-TS – Technician's What If's, Technicians' Morning Checklist and SBE Procedures for Election Day establish processes to protect against a single point of failure.		
O-5	SBE will maintain a record, as required by law, (Federal and State) of all original audit data that cannot be modified or overridden but may be	M	A process is in place to maintain a record, as required law, Federal and State of all original audit data that cannot be modified or overridden but may be augmented by designated authorized		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~augmented by designated authorized officials in order to adjust for errors or omissions (e.g., during the canvassing process).~~		~~officials in order to adjust for errors or omissions (e.g., during the canvassing process) as defined in the Election Judges Manual.~~		
~~O-6~~	~~SBE will ensure that a process is implemented that detects and records every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator.~~	~~M~~	~~The AccuVote-TS and GEMS software both detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator as described in Precinct Count 1.96 User's Guide, AccuVote System Guide and GEMS 1.18 User Guide to conform to state requirements in COMAR 33.10.02.10~~		
~~O-7~~	~~SBE will ensure that a process is implemented that maintains a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path.~~	~~M~~	~~The Procedures for Official Canvas, Verification and Post-Election Audit, Recount procedures; GEMS 1.18 Users Guide, and Election Judges Guide ensure a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path is maintained.~~		
~~O-8~~	~~SBE will ensure that a process is implemented to retrieve ballot images in a form readable by humans.~~	~~M~~	~~The Election Judges Guide describes the process that is used to ensure the ballot image is in a form readable by humans.~~		
~~O-9~~	~~SBE will ensure that all error messages requiring intervention by an operator or precinct~~	~~M~~	~~The Precinct Count 1.96 User's Guide covers all error messages requiring intervention by an operator or precinct~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~official shall be displayed or printed unambiguously in easily understood language text, or by means of other suitable visual indicators.~~		~~official displayed or printed is unambiguously in easily understood language text, or by means of other suitable visual indicators.~~		
~~O-10~~	~~SBE will ensure that a process is implemented for a security seal, a password, or a data code recognition capability to prevent the inadvertent or unauthorized actuation of the DRE Device.~~	~~P~~	~~If SBE does not ensure that a process is implemented for a security seal, a password, or a data code recognition capability to prevent the inadvertent or unauthorized actuation of the DRE device, then integrity of the DRE device may not be maintained resulting in the potential loss of system confidentiality, integrity, and availability.~~ ~~The AccuVote-TS Pre-Election Logic & Accuracy Testing and Checklist procedures ensure a security seal is placed on each DRE device. However, the key used to lock the PCMCIA card and printer on the DRE has a universal key (i.e., the same key for all DREs).~~ ~~**Likelihood: MEDIUM**~~ ~~With the number of Diebold DRE devices on the market it is likely that a key could become lost or stolen. However, the openness of the polling stations impedes the exploitation of this vulnerability.~~ ~~**Impact: MEDIUM**~~ ~~The impact of the exploitation of this vulnerability could impact multiple DRE devices, adversely impacting SBE's~~	~~**MEDIUM**~~	~~The key used to lock the PCMCIA card and the printer should be specific to individual DRE devices or groups of DRE devices or tamper-proof tape should be placed over the lock and/or access panel during the election.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			~~mission.~~		
~~O-11~~	~~SBE will implement procedures to establish and maintain controls that ensure that accidents, inadvertent mistakes, and errors are minimized.~~	~~M~~	~~The Technicians Election Day Check Lists; Tech's TS What If's; SBE Procedures for Election Day, and Election Judges Guidelines have been implemented to establish and maintain controls that ensure that accidents, inadvertent mistakes, and errors are minimized.~~		
~~O-12~~	~~SBE will implement procedures to protect the system from intentional manipulation and fraud, and from malicious mischief.~~	~~M~~	~~The AccuVote-TS Pre-Election Logic & Accuracy Testing and Checklist, Technicians Election Day Check Lists; Tech's TS What If's; SBE Procedures for Election Day, and Election Judges Guidelines have been implemented to establish and maintain controls that ensure effective procedures to protect the system from intentional manipulation and fraud, and from malicious mischief are followed.~~		
~~O-13~~	~~SBE will implement procedures to protect secrecy in the voting process.~~	~~M~~	~~The Election Judge and Polling officials follow procedures in the Election Judge's Manual to protect secrecy in the voting process.~~ ~~AccuVote-TS also ensures privacy because it does not use personal information.~~		
~~O-14~~	~~SBE will implement procedures to prevent unauthorized~~	~~P~~	~~If SBE does not implement procedures to prevent unauthorized changes to system~~	~~HIGH~~	~~SBE should replace the public FTP server with Secure Copy (SCP), Secure FTP~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	changes to system capabilities for defining ballot formats, casting and recording votes, calculating vote totals consistent with defined ballot formats, and reporting vote totals.		capabilities for defining ballot formats, casting and recording votes, calculating vote totals consistent with defined ballot formats, and reporting vote totals, then system confidentiality, integrity, and availability may be compromised. The AccuVote-TS Logic and Accuracy Testing procedures have been implemented to prevent unauthorized changes to system capabilities for defining ballot formats, casting and recording votes, calculating vote totals consistent with defined ballot formats, and reporting vote totals; however during the Ballot Creation Process the ballot is transferred to the LBEs via an FTP server. **Likelihood: HIGH** The ballot format can be modified either while in transit or while on the public FTP server. **Impact: HIGH** An attacker could use this server to change the initial ballot and possibly place Trojan software within the ballot data causing the validity and integrity of the election to be questioned. An FTP server is one of the most insecure ways to distribute files.		(sFTP), Secure Sockets Layer (SSL), or Transport Layer Security (TLS) to protect the ballot during transmission. SBE should encrypt the ballot while on the intermediate server to prevent unauthorized access to the file.
O-15	SBE will implement procedures to prevent the changing or	M	The Election Judge and Polling officials follow procedures in the Election Judge's		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~prevention of recording a vote.~~		~~Manual to prevent the changing or prevention of recording a vote. The DRE only allows the voter to cast one vote. Once a vote is cast, the Voter Access Card is deactivated and cannot be used again until reactivated by the election officials.~~		
~~O-16~~	~~SBE will implement procedures to prevent changing calculated vote totals.~~	~~M~~	~~The Election Judge and Polling officials follow procedures in the Election Judge's Manual to prevent changing calculated vote totals. The LBE officials follow Election Results Transfer Memorandum to prevent changing calculated vote totals. The SBE officials follow Election Results Transfer Memorandum and General Election Night Processing procedures to prevent changing calculated vote totals.~~		
~~O-17~~	~~SBE will implement procedures to prevent access to vote data, including individual votes and vote totals, to unauthorized individuals.~~	~~M~~	~~The Election Judges, Polling officials and technicians follow procedures in Technicians Election Day Check Lists; Tech's TS What If's, SBE Procedures for Election Day, and Election Judges Guidelines to prevent access to vote data, including individual votes and vote totals, to unauthorized individuals.~~		
~~O-18~~	~~SBE will implement a process to prevent access to voter identification data for votes cast by the voter such that an individual can determine the content of specific votes casts by the voter.~~	~~M~~	~~The Election Judges Manual establishes a process to prevent access to voter identification data for votes cast by the voter such that an individual can determine the content of specific votes casts by the voter.~~ ~~AccuVote-TS also ensures privacy~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~because it does not use personal information.~~		
~~O-19~~	~~SBE will implement procedures that require all systems that transmit data over public telecommunications networks to preserve the secrecy of a voter's ballot choices, and prevent anyone from violating ballot privacy.~~	~~M~~	~~As certified by the ITA, the DRE does not transmit individual ballot information.~~		
~~O-20~~	~~SBE will implement procedures that detect the occurrence of a telecommunication interruption at the poll site and switch to an alternative mode of operation that is not dependent on the connection between the poll site voting devices and external system components.~~	~~M~~	~~The Elections Judges Manual and Election Administrator's Guide establishes procedures to detect the occurrence of a telecommunication interruption at the poll site and switch to an alternative mode of operation that is not dependent on the connection between the poll site voting devices and external system components.~~		
~~O-21~~	~~SBE will implement procedures to provide an alternate voting mode without the voter losing their ability to vote.~~	~~M~~	~~The provisional ballot process outlined in the Election Judges Manual provides an alternate voting mode without the voter losing their ability to vote.~~		
~~O-22~~	~~Emergency procedures should be put in place for contingencies such as equipment failure or malicious activity that could make the voting systems unavailable.~~	~~M~~	~~The SBE Disaster Recovery and Incident Management Plan are in place for contingencies such as equipment failure or malicious activity that could make the voting systems unavailable.~~		
~~O-23~~	~~SBE shall implement procedures that will protect the DRE units from unauthorized~~	~~N/A~~	~~The DRE voting terminals are not connected to communications lines during the election.~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~access via communications lines.~~		~~during the election.~~		
~~O-24~~	~~SBE shall implement procedures that will protect the DRE units from unauthorized access via wireless communications.~~	~~N/A~~	~~The DRE units are not connected to wireless communications.~~		
~~O-25~~	~~All electronic information shall be backed up as appropriate and secured from unauthorized access.~~	~~M~~	~~All electronic information is backed up where appropriate and secured from unauthorized access as defined in the Election Judges Manual and the State-Wide Voting System Project General Election Results Export Procedures.~~		
~~O-26~~	~~Upon learning of a possible incident, SBE needs to take steps to verify that the incident actually does exist.~~	~~M~~	~~Upon learning of a possible incident, the SBE follows steps within the Disaster Recovery and Incident Management Plan to verify that the incident actually does exist.~~		
~~O-27~~	~~Once the incident is verified, its scope should be determined.~~	~~M~~	~~Once the incident is verified, its scope is determined by following the Disaster Recovery and Incident Management Plan.~~		
~~O-28~~	~~When apprising users of the existence of an incident, SBE should make every attempt to provide clear and concise information.~~	~~M~~	~~When apprising users of the existence of an incident, SBE follows the Disaster Recovery and Incident Management Plan to make every attempt to provide clear and concise information.~~		
~~O-29~~	~~SBE must accurately record and report the defects in vendor-provided software products to the proper vendors~~	~~M~~	~~The Quality Assurance (QA) Plan and Risks, Issues, Systems Incidents, and Changes (RISC) Plan accurately record and report the defects in vendor-provided~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	~~and, to user groups. The reports must be held confidential and reported to the proper vendor(s) in a timely manner.~~		~~software products to the proper vendors and, to user groups. The reports held confidential and reported to the proper vendor(s) in a timely manner.~~		
~~O-30~~	~~SBE shall comply with all intellectual property, copyright, patent, or trade secret issues.~~	~~M~~	~~SBE complies with all intellectual property, copyright, patent, or trade secret issues as stated in the contract with vendor.~~		
~~O-31~~	~~If SBE possesses source code or has made non-disclosure agreements, care should be taken to avoid revealing any information that is legally protected.~~	~~N/A~~	~~The SBE does not possess source code. SBE complies with non-disclosure agreements.~~		
~~O-32~~	~~Incident logging should be treated much the same as evidence gathering: the incident log should be detailed, accurate, and the proper procedures should be followed so that the incident log could be used as evidence in a court of law.~~	~~U~~	~~If incident logging is not treated the same as evidence gathering, then legal requirements for chain of custody may not be met resulting in the inability to prosecute and/or unrecoverable financial loss.~~ ~~SBE does not have detailed evidence gathering procedures or processes.~~ ~~**Likelihood: LOW**~~ ~~The possibility of an attacker to gain access to a DRE source code for malicious activity is unlikely in its current configuration. The possibility of an attacker to gain access to a GEMS server for malicious activity is also~~	~~**LOW**~~	~~Establish procedures to preserve the incident logs on the DREs and the GEMS server and incorporate additional logging so that these logs may be used as evidence in a court of law.~~

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~unlikely in its current configuration.~~ ~~**Impact: LOW**~~ ~~Although incident logging is performed on the DREs and the GEMS server, there are no procedures established regarding these incident logs so they could be used as evidence in a court of law.~~		
~~O-33~~	~~After an incident has been resolved, a review should be conducted so that SBE can learn from the experience and, if necessary, update its procedures.~~	~~M~~	~~The Disaster Recovery and Incident Management Plan covers the process after an incident has been resolved, regarding reviews and updates to procedures.~~		
~~O-34~~	~~The security features of an IT system must be configured (e.g., enabled or disabled) to meet the needs of a specific installation and to account for changes in the operational environment.~~	~~U~~	~~If the security features of an IT system are not configured (e.g., enabled or disabled) to meet the needs of a specific installation and to account for changes in the operational environment, then security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system may be compromised. Some of the security services of the IT system are provided by the software itself. Buffer overflows and unchecked file locations could provide system level access to the OS.~~ ~~The following software vulnerabilities were found in the AccuVote-TS voting system source code.~~	~~**MEDIUM**~~	~~For the memcpy, tcscpy sscanf, and lstrcpy functions, ensure that the bounds of the receiving buffers are checked before the operation begins, and that operations cease when the buffer is full.~~ ~~Use more secure functions to acquire random numbers, such as mt_rand, which is faster than the average libc and can be used with cryptography.~~ ~~Declare necessary variables as constant to ensure that they could not be changed by malicious activities.~~ ~~When creating static arrays and variable declarations, ensure that the size allocated is larger than the maximum~~

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~The memcpy, tcscpy, sscanf, and lstrcpy functions do not check the size of the receiving variable, making them vulnerable to a buffer overflow.~~ ~~The srand function is not secure in its implementation of acquiring random numbers.~~ ~~Sprintf and vsprintf formatting is not declared as a constant, which would prevent changes to a variable.~~ ~~There are many static variable declarations used which could be utilized in a buffer overflow.~~ ~~No paths were used to designate external library files, allowing possible trojans to be introduced.~~ ~~The system function is used which allows for shell execution of the passed parameter.~~ ~~The crypt function is used for a one-way hash, this function is vulnerable to a dictionary based, brute force attack.~~ ~~Race conditions exist for temporary file accesses, this could allow for a file substitution which could lead to unauthorized access.~~ ~~The open function is used to open files. This does no checking for valid files, and~~		~~possible length.~~ ~~Specify paths to external library files by using registry entries or other verifiable system variables.~~ ~~Do not use shell execution methods without extensive checking of the passed parameter to defend against trojaned operation.~~ ~~The crypt function is an outdated method for creating a cryptological hash. Use SHA-1 for a more secure hash.~~ ~~Race conditions can be avoided programmatically so that no two calls reference the same resource at the same time.~~ ~~Perform validation checking before doing any file operations.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			symlinks or shortcuts could be used to open device files or data outside the scope of this function. **Likelihood: MEDIUM** These findings are mitigated by the fact that the DREs are not connected to a network and by the openness of the voting environment. **Impact: HIGH** An attacker could use these vulnerabilities to gain full access to the voting system, invalidating any other security controls, and allowing access to the or possible alteration of the voting results.		
O 35	It is essential to detect security breaches (e.g., network break-ins, suspicious activities) so that a response can occur in a timely manner.	U	If security breaches (e.g., network break-ins, suspicious activities) are not detected so that a response can occur in a timely manner, then mitigation efforts may be after the fact resulting in loss of system confidentiality, integrity, and availability. SBE does not detect security breaches. **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	**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~~
			~~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.~~		
~~O-36~~	~~Security responsibility should be assigned to ensure that adequate security is provided for the mission-critical IT systems.~~	~~M~~	~~The Election Judge Manual and the Technician Guide assign responsibility to ensure that adequate security is provided for the mission-critical IT systems. This function is performed by LBE and precinct staff.~~		
~~O-37~~	~~Personnel security controls, including separation of duties, least privilege, and user computer access registration and termination should be implemented.~~	~~M~~	~~The Election Judges Manual, and Election Administrator's Guide establishes personnel security controls, including separation of duties, least privilege, and user computer access registration and termination. This function is performed by LBE and precinct staff.~~		
~~O-38~~	~~Security awareness and technical training should be conducted to ensure that end users and system users are aware of the rules of behavior and their responsibilities in protecting the organizations mission. This training will include information about threats, risks and vulnerabilities~~	~~U~~	~~If security awareness and technical training is not conducted to ensure that end users and system users are aware of the rules of behavior and their responsibilities in protecting the organization's mission, then security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system may be compromised.~~	~~**HIGH**~~	~~Training should be established for security awareness and technical training to ensure that system users are aware of the rules of behavior and their responsibilities in protecting the organizations mission. This training should include information about threats, risks, vulnerabilities, and risks to voting systems.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	to voting systems, and the need to protect them.		may be compromised. Security awareness and technical training is not conducted to ensure that end users and system users are aware of the rules of behavior and their responsibilities in protecting the organizations mission. The SBE has training for all of the election judges, poll workers and technicians. However, this training does not adequately address security issues. **Likelihood: HIGH** Without security awareness training the election judges, poll workers and technicians may not be aware of their security responsibilities. **Impact: HIGH** If the vulnerability is exploited the validity and integrity of the election process may be compromised.		
O 39	Periodic testing of security controls should be conducted to ensure that the controls are effective.	U	If periodic testing of security controls is not conducted to ensure that the controls are effective, then unplanned risks may be introduced to the system and the existing security controls may be circumvented and the confidentiality, integrity, and availability of the system may be compromised. Periodic security testing is not performed	**LOW**	Implement a periodic security testing program to ensure that the system security controls remain effective over time.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			for the AccuVote-TS voting system. **Likelihood: LOW** The risk assessment process is an effective control for baselining the existing security controls and the system risks. **Impact: HIGH** If the vulnerability is exploited the validity and integrity of the election process may be compromised.		
O-40	Periodic system audits should be performed.	M	Periodic system audits are performed using the Logic and Accuracy Plan and the Procedures for Official Canvass, Verification and Post-Election Audit.		
O-41	Continuity of support should be provided, and a continuity of operations plan should be developed, tested, and maintained to provide for business resumption and ensure continuity of operations during emergencies or disasters.	M	A Continuity of Operations plan has been developed, tested, and maintained in the Disaster Recovery and Incident Management Plan and the Emergency Continuity Plan. An inventory of backup DREs is maintained at the LBE. The SBE maintains a backup GEMS server at the State of Maryland Archives building. In addition, Diebold has a warehouse of DRE devices located at BWI airport.		
O-42	An incident response capability should be developed to prepare for, recognize, report, and respond to the incident and return the IT system to operational status.	M	The Disaster Recovery and Incident Management Plan and the Emergency Continuity Plan establish an incident response capability to prepare for, recognize, report, and respond to the incident and return the IT system to		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~operational status.~~		~~operational status.~~		
~~O-43~~	~~To ensure consistency and uniformity in security operations, step-by-step procedures and methods for implementing (preventive and detection) operational controls must be clearly defined, documented, and maintained.~~	~~U~~	~~If step-by-step procedures and methods for implementing (preventive and detection) operational controls are not clearly defined, documented, and maintained, then security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system may be compromised.~~ ~~No security operations, step-by-step procedures and methods for implementing (preventive and detection) operational controls is defined, documented, and maintained. Therefore, operational controls may be implemented inconsistently, incorrectly, and incompletely. Interviews with system personnel indicated that security functions were being performed.~~ ~~**Likelihood: LOW**~~ ~~The absence of consistent and uniform security controls may lead to unauthorized, undetected, or unknown changes to system settings. This vulnerability can be exploited by all human threats, but due to other existing physical and technical security controls this has been rated low.~~ ~~**Impact: HIGH**~~ ~~The exploitation of a GEMS server may~~	~~**LOW**~~	~~To ensure consistency and uniformity in security operations, step-by-step procedures and methods for implementing (preventive and detection) operational controls must be clearly defined, documented, and maintained by the SBE and LBE.~~

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~cause the validity and integrity of the voting process to be compromised.~~		
~~O-44~~	~~The person responsible for voting system contingency planning must be aware of risks to the system and recognize whether the current contingency plan is able to address residual risks completely and effectively.~~	~~M~~	~~The personnel responsible for voting system contingency planning are aware of risks to the system and recognize whether the current contingency plan is able to address residual risks completely and effectively as shown in the Emergency Contingency Plan and the Disaster Recovery and Incident Management Plan.~~		
~~O-45~~	~~There should be coordination between each IT Contingency plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.~~	~~N/A~~	~~There are no interconnections to other systems. Therefore, there is not a requirement for coordination between multiple contingency plans.~~		
~~O-46~~	~~Organizations should prepare their internal and external communications procedures prior to a disaster.~~	~~M~~	~~The SBE has an established Disaster Recovery and Incident Management Plan and Emergency Contingency Plan.~~		
~~O-47~~	~~Contingency measures should be identified and integrated at all phases of the computer system life cycle.~~	~~M~~	~~The Risks, Issues, System Incidents and Changes (RISC) Plan and SBE AccuVote Touch Screen Voting System, Phase II Implementation Plan satisfy contingency measures identified and integrated at all phases of the computer system life cycle.~~		
~~O-48~~	~~Contingency planning requirements should be considered when a new~~	~~M~~	~~SBE AccuVote Touch Screen Voting System, Phase II Implementation Plan has procedures for risk management~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~process is being conceived.~~		~~planning identification to be considered.~~		
~~O-49~~	~~Contingency strategies should be tested (in the implementation phase) to ensure that technical features and recovery procedures are accurate and effective. Testing on an ongoing basis, as necessary, shall be conducted to ensure that procedures continue to be effective.~~	~~N/A~~	~~The system is not in the implementation phase.~~		
~~O-50~~	~~Backups should be stored offsite.~~	~~U~~	~~If backups are not stored offsite, then a disaster may destroy both the original and backup data copy making system recoverability difficult or impossible.~~ ~~The systems, PCMCIA cards, and paper backups are all stored at the same location. Therefore, a disaster at the storage facility could destroy all the voting records from the election.~~ ~~**Likelihood: LOW**~~ ~~Existing physical controls at the storage facility mitigate the likelihood.~~ ~~**Impact: LOW**~~ ~~The canvassing process is completed prior to the final storage of the PCMCIA cards and paper backups, therefore the impact of the loss would be minimal.~~	~~**LOW**~~	~~Implement a procedure for storing backups offsite.~~

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
~~O-51~~	~~When the IT system undergoes upgrades or any other modifications, such as changes to external interfaces, these modifications should be reflected in the contingency plan, in a timely manner.~~	~~M~~	~~The Disaster Recovery and Incident Management Plan has procedures to reflect upgrades and any other modifications, such as changes to external interfaces to the DRE and GEMS server.~~		
~~O-52~~	~~Until a new system is operational and fully tested (including its contingency capabilities), the original system's contingency plan should be ready for implementation.~~	~~N/A~~	~~The AccuVote-TS voting system is in the operational and maintenance phase of its life cycle. It is not undergoing replacement.~~		
~~O-53~~	~~The contingency planning policy statement should define the SBE's overall contingency objectives and establish the organizational framework and responsibilities for IT contingency planning.~~	~~M~~	~~The Disaster Recovery and Incident Management Plan defines the SBE's overall contingency objectives and establish the organizational framework and responsibilities for IT contingency planning.~~		
~~O-54~~	~~SBE officials must support the Contingency Planning process and should be included in the process to develop the program policy, structure, objectives, and roles and responsibilities.~~	~~M~~	~~SBE officials support the Contingency Planning process and have been included in the process to develop the program policy, structure, objectives, and roles and responsibilities.~~		
~~O-55~~	~~As the IT contingency policy and program are developed, they should be coordinated with related SBE activities, including IT security, physical security,~~	~~M~~	~~The IT contingency policy and program are developed, and are coordinated with related SBE activities, including IT security, physical security, human resources, IT operations, and emergency~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~human resources, IT operations, and emergency preparedness functions.~~		~~preparedness functions.~~		
~~O-56~~	~~Contingency plans must be written in coordination with other existing plans associated with systems.~~	~~M~~	~~Contingency plans have been written in coordination with other existing plans associated with the system.~~		
~~O-57~~	~~Preventive controls should be documented in the contingency plan, and personnel associated with the system should be trained on how and when to use the controls.~~	~~M~~	~~Preventive controls are documented in the Election Judge Manual, and personnel associated with the system are trained on how and when to use the controls.~~		
~~O-58~~	~~Preventive controls should be maintained in good condition to ensure their effectiveness in an emergency.~~	~~M~~	~~Preventive controls are maintained in good condition to ensure their effectiveness in an emergency.~~		
~~O-59~~	~~Procedures should specify the frequency of backups (e.g., daily or weekly, incremental or full), based on data criticality and the frequency that new information is introduced.~~	~~M~~	~~The Election Judges Manual and General Election Results Export Procedures provides steps for backups of data.~~		
~~O-60~~	~~Data backup documentation should designate the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite.~~	~~M~~	~~The Election Judges Manual and General Election Results Export Procedures designate the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite.~~		
~~O-61~~	~~The specific method chosen for conducting backups should be~~	~~M~~	~~The Election Judges Manual and General Election Results Export~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~based on system and data availability and integrity requirements.~~		~~Procedures establish several methods to backup the data, including hard copy, magnetic media and central standalone server.~~		
~~O-62~~	~~The contingency plan must include a strategy to recover and perform system operations at an alternate facility for an extended period.~~	~~M~~	~~The Disaster Recovery and Incident Management Plan and Emergency Contingency Procedure include a strategy to recover and perform system operations at an alternate facility for an extended period.~~		
~~O-63~~	~~The alternate facility chosen must be able to support system operations as defined in the contingency plan.~~	~~M~~	~~The Disaster Recovery and Incident Management Plan and Emergency Contingency Procedure choose alternate facilities capable to support system operations as defined in the contingency plan.~~		
~~O-64~~	~~Alternate site selection of fixed-site locations should account for the time and mode of transportation necessary to move personnel there.~~	~~M~~	~~The Disaster Recovery and Incident Management Plan and Emergency Contingency Procedure take into account for the time and mode of transportation necessary to move personnel there when selecting an alternate site selection.~~		
~~O-65~~	~~The alternate fixed site should be in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure) as the organization's primary site.~~	~~M~~	~~The Disaster Recovery and Incident Management Plan and Emergency Contingency Procedure considers geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure) as the organization's primary site when choosing an alternate site.~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
O-66	Contingency test results and lessons learned shall be documented and reviewed by test participants and other personnel as appropriate.	M	The Disaster Recovery and Incident Management Plan and Emergency Contingency Procedure has established process for contingency testing and lessons learned.		
O-67	A copy of the contingency plan shall also be stored at the alternate site and with the backup media.	M	Each LBE as well as the SBE has a copy of the Disaster Recovery and Incident Management Plan and Emergency Contingency Procedure.		
O-68	The Contingency Planning Coordinator should maintain a record of copies of the plan and to whom they were distributed.	U	If the Contingency Planning Coordinator does not maintain a record of copies of the plan and to whom they were distributed, then outdated plans may be in circulation, which may impact recovery in the event of a disaster. A record of copies of the plan and to whom they were distributed is not maintained. Therefore it is possible for outdated plans to remain in circulation. **Likelihood: LOW** A small number of officials are responsible for coordinating contingency plans are their implementation. These responsible individuals are in constant communication during an election. **Impact: LOW** Activation of contingency plan could be delayed because the contingency planning coordinator may have an	**LOW**	A record of copies of the contingency plan should be maintained by SBE and LBE.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			outdated contact list.		
O-69	Other information that should be stored with the contingency plan includes contracts with vendors (SLAs and other contracts), software licenses, system users' manuals, security manuals, and operating procedures.	M	Along with the contingency plan, LBEs have copies of the relevant documentation and produced the documentation on request.		
O-70	The Contingency Planning Coordinator should record plan modifications using a Record of Changes, which lists the page number, change comment, and date of change.	M	The Risks, Issues, Systems Incidents, and Changes (RISC) Plan is used to record plan modifications.		
O-71	The Contingency Planning Coordinator should coordinate frequently with associated internal and external organizations and system POCs to ensure that impacts caused by changes within either organization will be reflected in the contingency plan.	M	The Disaster Recovery and Incident Management Plan has established a requirement to update plan at least once a year. As part of this update, the Contingency Planning Coordinator interacts with internal and external organizations and POCs.		
O-72	Strict version control must be maintained.	M	The Disaster Recovery and Incident Management Plan has strict version control implemented.		
O-73	The Contingency Planning Coordinator should evaluate supporting information to ensure that the information is	M	The Disaster Recovery and Incident Management Plan has procedures to evaluate supporting information to ensure that the information is current and		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	current and continues to meet system requirements adequately.		continues to meet system requirements adequately.		
O-74	Damage assessment procedures should be developed for the voting system.	M	The Disaster Recovery and Incident Management Plan has procedures to assess the damage of the voting system.		
O-75	Personnel with damage assessment responsibilities should understand and be able to perform these procedures in the event the paper plan is unavailable during the situation.	M	Election Judges and system technicians, who have damage assessment responsibilities, are given training to understand and be able to perform these procedures in the event the paper plan is unavailable during the situation.		
O-76	The IT contingency plan should be activated by the appropriate authority only when the damage assessment indicates that one or more of the activation criteria for that system are met.	M	The Disaster Recovery and Incident Management Plan has an escalation procedure and activation criteria determined by the damage assessment results.		
O-77	Teams with recovery responsibilities should understand and be able to perform these recovery strategies well enough that if the paper plan is unavailable during the initial stages of the event, they can still perform the necessary activities.	N/A	This requirement is outside of the scope of this assessment. If teams with recovery responsibilities do not understand and are not able to perform these recovery strategies well enough that if the paper plan is unavailable during the initial stages of the event, then plan execution may be incomplete or inaccurate.		
O-78	Recovery procedures should reflect system priorities	U	If recovery procedures do not reflect system priorities identified in the	LOW	Ensure the Business Impact Analysis (BIA) identifies critical IT resources, single

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	~~identified in the Business Impact Analysis.~~		~~Business Impact Analysis, then critical systems may not be recovered first.~~ ~~A Business Impact Analysis identifies system priorities and the impact they have on the voting process. A Business Impact Analysis has not been performed.~~ ~~**Likelihood: LOW**~~ ~~Other system controls such as the Disaster Recovery and Incident Response Plan list recovery priorities.~~ ~~**Impact: LOW**~~ ~~Recovery priorities may not be optimized.~~		~~points of failure, internal and external POC associated with the system, develops recovery priorities, and determines disruption impacts and allowable outage times.~~ ~~Ensure procedures for identifying, selecting, installing, and modifying system software are also addressed by the BIA.~~
~~O-79~~	~~The contingency plan should provide detailed procedures to restore the IT system or system components. To prevent difficulty or confusion in an emergency, no procedural steps should be assumed or omitted~~	~~M~~	~~The Disaster Recovery and Incident Management Plan have established procedures to restore the IT system or system components. To prevent difficulty or confusion in an emergency, no procedural steps are assumed or omitted.~~		
~~O-80~~	~~Procedures should be assigned to the appropriate recovery team.~~	~~M~~	~~The Disaster Recovery and Incident Management Plan has established recovery team assignments.~~		
~~O-81~~	~~Until the primary system is restored and tested, the contingency system should continue to be operated.~~	~~M~~	~~The Disaster Recovery and Incident Management Plan has procedures to continue the use of contingency system.~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
O-82	The Reconstitution Phase should specify teams responsible for restoring or replacing both the site and the IT system.	M	The Disaster Recovery and Incident Management Plan has established procedures on System and Facility Recovery.		
O-83	In addition to backing up data, organizations should also back up system device drivers.	U	If in addition to backing up data, organizations do not also back up system device drivers, then systems may not be fully recoverable. Backup of device drivers is not performed. When device drivers are not backed up, restoration of the system is impeded. **Likelihood: LOW** The likelihood of needing device driver backups is low because the device drivers are contained in the OS. **Impact: LOW** The impact is low because the device drivers can be restored from the OS.	**LOW**	Backup device drivers in addition to other data.
O-84	It is important that media be retrieved on a regular basis from off-site storage and tested to ensure that the backups are being performed correctly.	N/A	Data is only stored as required by law for post election audit and challenges to an election (maximum of 22 months).		
O-85	Each backup tape, cartridge, or disk should be uniquely labeled, including a date, to ensure that the required data can be	N/A	Data is only stored as required by law for post election audit and challenges to an election (maximum of 22 months).		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	the required data can be identified quickly in an emergency.				
O-86	If remote access is established as a contingency strategy: (1) Data bandwidth requirements should be identified and used to scale the remote access solution; (2) Security controls such as one-time passwords should be considered; and, (3) Data encryption should be implemented if the communications contains sensitive information.	N/A	Remote access is not supported in the contingency strategy.		
O-87	Security patches should be tested to check for any unintended consequences on configuration or software specific to the organization.	M	The ITA recertifies any patches or upgrades of the systems. An Acceptance and Accuracy Test and Certification are then performed by the SBE and the LBE performs a Logic and Accuracy Test and Certification before the patches or upgrades are accepted for use.		
O-88	All unneeded default accounts and groups should be removed to eliminate their use by intruders, including guest accounts on computers containing sensitive information.	M	All unneeded default accounts and groups are removed to eliminate their use by intruders, including guest accounts on computers containing sensitive information. Needed default accounts are in use and should be closed and replaced with non-		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			default accounts.		
O-89	To prevent alteration of executable code, no software shall be permanently installed or resident in the system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.	U	If the alteration of executable code is allowed, then unplanned risks may be introduced to the system and the existing security controls may be circumvented and the confidentiality, integrity, and availability of the system may be compromised. SBE receives all software and firmware and software directly from the ITA. SBE, in turn, instructs the vendor what version to load on systems. With this arrangement, the vendor can load uncertified software on to the system without SBE's knowledge. **Likelihood: HIGH** The vendor has a contractual obligation to load only certified software, but there are no controls to ensure this occurs. **Impact: HIGH** An uncertified version may contain malicious code, which could compromise the integrity of the voting process.	**HIGH**	SBE should verify correct firmware and software version prior to use.
O-90	After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible on the voting system.	M	The ITA has verified no source code or compilers or assemblers shall be resident or accessible on the voting system.		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
O-91	System and procedures must ensure that each voter can vote only once.	M	The Logic and Accuracy Test and Certification procedures check that each voter can vote only once. Also, the DRE only allows the voter to cast one vote. Once a vote is cast, the Voter Access Card is deactivated and can not be used again until reactivated by the election officials.		
O-92	End user access to the system is provided only through the approved interface.	M	The Election Judge Manual sets procedures for voter access to the system is provided only through the approved interface. The voter must verify their identity by the Book Election Judge and be given a Voter Authority Card before allowed access to the Voting Unit Access Judge. Once the voter is at the Voting Unit Access Judge, the voter must relinquish his Voter Authority Card and receive an activated Voter Access Card. The voter interfaces with the DRE voting terminal only through the touch screen interface. The DRE does not have any infrared ports or exposed communications ports to facilitate unauthorized access to the terminal.		
O-93	Process is in place to apply appropriate security patches to maintain a secure configuration.	U	If processes are not in place to apply appropriate security patches to maintain a secure configuration, then the existing security controls may be circumvented and the confidentiality, integrity, and availability of the system may be compromised. A process is not in place to apply	**MEDIUM**	Create and implement a formal process to ensure that the voting system is up to date with all applicable patches.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~security patches in order to maintain a secure configuration.~~ ~~**Likelihood: MEDIUM**~~ ~~Implementation of security patches ensures system stability and availability. Two high vulnerabilities were discovered on the GEMS server, however due to the existing operational and physical security controls this risk likelihood is rated medium.~~ ~~**Impact: HIGH**~~ ~~A malicious user could use these vulnerabilities to gain complete system control either locally or remotely. Additionally, without these security patches, the system may become unavailable.~~		